MultiAccess™
Communications Server

MA30120

User Guide

MultiTech® Systems

User Guide

MultiAccess Communications Server
MultiAccess
S000255D Revision D

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc.

Copyright © 2006 by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Date	Description
A	11/17/03	Manual released.
B	12/06/04	Manual revised to include an appendix on modem commands and version 1.08 of the MultiAccess software.
C	07/05/05	Manual revised to include software release version 1.12.
D	10/04/06	Manual revised to update AT Commands in Appendix B and includes software version 1.14.

Patents

This device covered by one or more of the following patents: 6,031,867; 6,012,113; 6,009,082; 5,864,560; 5,815,503; 5,812,534; 5,790,532; 5,764,628; 5,764,627; 5,754,589; 5,724,356; 5,673,268; 5,673,257; 5,628,030; 5,619,508; 5,617,423; 5,600,649; 5,592,586; 5,577,041; 5,574,725; 5,559,793; 5,546,448; 5,546,395; 5,535,204; 5,500,859; 5,471,470; 5,463,616; 5,453,986; 5,452,289; 5,450,425; 5,309,562; 5,301,274

Trademarks

Trademarks of Multi-Tech Systems, Inc.: Multi-Tech, and Multi-Tech logo.
HylaFAX is a trademark of Silicon Graphics Corporation. Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
All products or technologies are the trademarks or registered trademarks of their respective holders.

Technical Support

Country	By Email	By Phone
France:	support@multitech.fr	+(33) 1-64 61 09 81
India:	support@multitechindia.com	+91 (124) 2340780
Europe, Asia, Africa:	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others:	support@multitech.com	(800) 972-2439 or +763-717-5863

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Internet Address: http://www.multitech.com

Contents

Chapter 1 - Introduction and Description 5

WAN Communications 5
Management 5
Remote Access 5
Features 6
Ship Kit Contents 6
Front Panel 7
Back Panel 8
Typical Application 9
Specifications 11

Chapter 2 - Installation 12

Safety Warnings 12
Safety Recommendations for Rack Installations 12
Site Planning 13
Hardware Installation Procedure 14
Starting Your MultiAccess 15
Network Setup 19
Line Interfaces 20
Modem Setup 21
User Authentication 28

Chapter 3 - Software 32

Home and Logout Options 33
Administration 35
Networks & Services 50
Network Setup 56
DHCP Server 66
Tracking 70
Packet Filters 71
User Authentication 75
Modem Setup 88
Statistics & Logs 98
Line Interfaces 117

Chapter 4 - Troubleshooting 129

Chapter 5 - MultiAccess Maintenance 130

Chapter 6- Warranty and Service 131

Regulatory Compliance 133
Recording MultiAccess Information 135

Appendix A - License Agreements 136

GNU GENERAL PUBLIC LICENSE 138

Appendix B – Modem Commands 141

“AT” Command Syntax Convention 141
“AT” Commands Supported 144

"AT" Commands Accepted with No Effect 147
S-Registers 148
Advanced MultiAccess Modem Commands 152
Application Notes 159
ASCII Conversion Chart 161

Appendix C – How to Update 162

Menu Driven: 162
Manual Method (via Linux command line): 162

Appendix D – Waste Electrical and Electronic Equipment (WEEE) Statement 165

Glossary 166

Index 177

Chapter 1 - Introduction and Description

Welcome to Multi-Tech's new MultiAccess Communications Server, Model MultiAccess. The MultiAccess Communications Server is a high-performance digital remote access solution for Enterprise LANs and Intranets or Internet service providers. MultiAccess is a V.92 remote access server (RAS) supporting up to four T1 line interfaces implementing either RBS or PRI signaling for use in North America or up to four E1 line interfaces implementing PRI signaling for the rest of the world. The MultiAccess Communications Server uses a web based Graphical User Interface (GUI) for configuration, is a 1U (one-up) rackmountable unit that contains up to four universal modem ports for dial-in communications.

WAN Communications

MultiAccess ships turnkey for T1/RBS or T1/E1 PRI ISDN and populated with 30 modems on line interface 1 for the basic configuration. Additional modem modules can be added to support up to four T1/E1 line interfaces. The high-density modems provide V.92/56K dial-up speeds. In addition, they are manageable from remote locations using platform-independent, industry standard protocols.

Management

MultiAccess includes robust management support allowing a network administrator to securely manage the devices either through a web browser or at the command line. The browser-based option uses the HTTPS protocol, also know as SSL (Secure Sockets Layer) to provide 128-bit encryption to secure the management session. The command line interface is accessible via SSH (Secure Shell) and supports SCP (Secure Copy) and sftp (Secure File Transfer Protocol) to help provide maintenance support.

SNTP Support. MultiAccess includes an industry standard Simple Network Time Protocol (SNTP) client that enables it to synchronize its clock with a remote time/clock server on the Internet. This feature is useful for accounting purposes.

Remote Access

Comprehensive Security. MultiAccess provides an industry standard Radius Server and Radius Client for authentication and authorization of thousands of user profiles using PAP and CHAP. In addition, it uses Network Address Translation (NAT) to hide internal, non-routable IP addresses. If a Radius Server does not exist, one is provided as part of the MultiAccess system. This Radius Server could provide authentication and authorization information for this and other Radius Clients in use at your site.

Features

- Compact design that supports up to four channelized T1 and/or IDSN PRI interfaces per rack unit
- Dial-in scalability for up to 96/120 users
- Terminates both analog and digital (ISDN) calls
- Client authentication provided through industry standard Radius®
- V.92 modem-on-hold
- V.92 quick connect
- V.44 data compression
- 10/100 Mb Ethernet Lan/Wan connectivity
- Simultaneous V.92/56K and 128 BRI ISDN sessions
- Industry-standard PPP client support
- PAP and CHAP authentication
- Secure, graphical local or remote management using HTTPS or SSH
- Standard 19” rackmountable chassis (1U)
- Two-year warranty

Ship Kit Contents

The MultiAccess is shipped with the following:

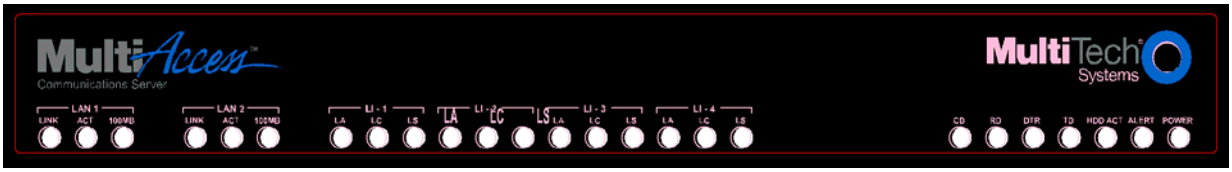
- 1 MultiAccess
- 4 power cords (US, Euro, Austral, & UK)
- 1 printed Quick Start Guide
- 1 Document CD
- 1 Recovery Image CD
- 2 Rack Mounting Brackets and four mounting screws

If any of these items are missing, contact Multi-Tech Systems or your dealer or distributor. Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the MultiAccess. Contact Multi-Tech’s Tech Support for advice.

Front Panel

The front panel has 16 front panel LEDs that provide operating status.

The Front Panel



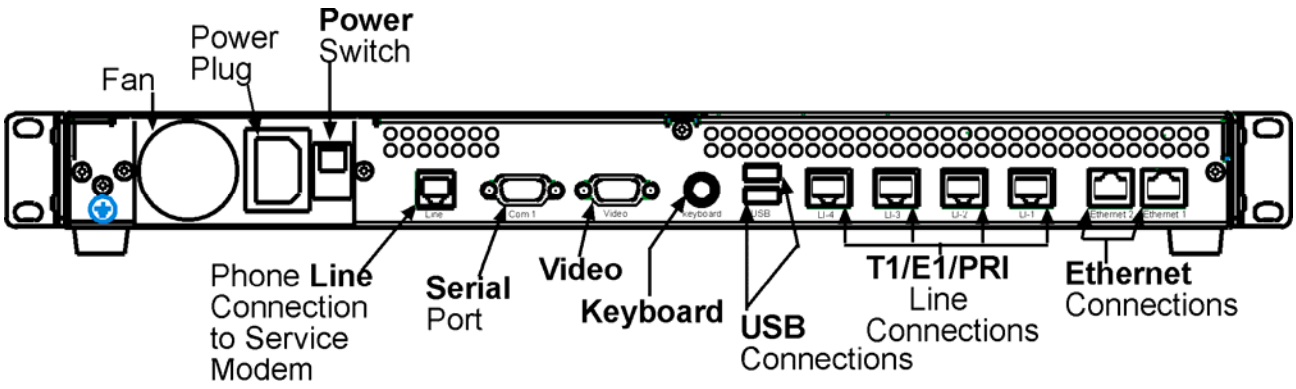
Front Panel LED Descriptions

LED	Description of LAN 1 & 2 LEDs
LINK	The LINK LED indicates link integrity for the LAN Ethernet port. If the Ethernet link is valid at either 10 Mbps or 100 Mbps, the LINK LED is lit. If the Ethernet link is invalid, the LINK LED is off.
ACT	The ACT (Activity) LED indicates either transmit or receive activity on the LAN Ethernet port. When activity is present on the LAN Ethernet port, the ACT LED is lit. When no activity is present on the LAN Ethernet port, the ACT LED is off.
100MB	The 100MB LED indicates the speed of the LAN Ethernet port. The 100MB LED is lit if the LAN Ethernet port is linked at 100 Mbps. The 100 MB LED is off at 10 Mbps.
LED	**Description of LIne LI-1 thru LI-4 LEDs**
LA	The LA (Link Active) indicates layer 1 is up. LA blinks when Los of Frame Alignment (LFA) but not Loss of Signal (LOS).
LC	The LC indicates a red alarm.
LS	The LS indicates a yellow alarm.
LED	**Description of Support Modem LEDs**
CD	The CD (Carrier Detect) LED lights when the modem detects a valid carrier signal from another modem. It is on when the modem is communicating with the other modem. It is off when the link is broken.
RD	The RD (Read Data) LED flashes when the modem is receiving data from another modem.
DTR	The DTR (Data Terminal Ready) LED lights when the operating system detects and initializes the modem.
TD	The TD (Transmit Data) LED flashes when the modem is transmitting data to another modem.
LED	**Description of System LEDs**
HDD ACT	The HDD ACT (Hard Disk Drive Activity) LED lights when the MultiAccess hard disk drive is accessed.
ALERT	The ALERT LED lights and the system beeps when memory DIMM is bad, missing, or if other rudimentary hardware failure.
POWER	The POWER LED is off when the MultiAccess is in a reset state. When the POWER LED is lit, the MultiAccess is not in a reset state.

Back Panel

The MultiAccess back panel has a fan, a power plug, the **POWER** Switch (**| / O**), an RJ-11 phone **LINE** jack, a DB-9 **COM1** jack, a DB-15 High-density DSUB (**VIDEO**) jack, two **USB** (Revision 1.1 compliant) jacks, four RJ-45 **T1/E1/PRI** line jacks, and two **Ethernet** RJ-45 (Ethernet 1 & Ethernet 2) jacks.

The MultiAccess back panel is illustrated and described below.

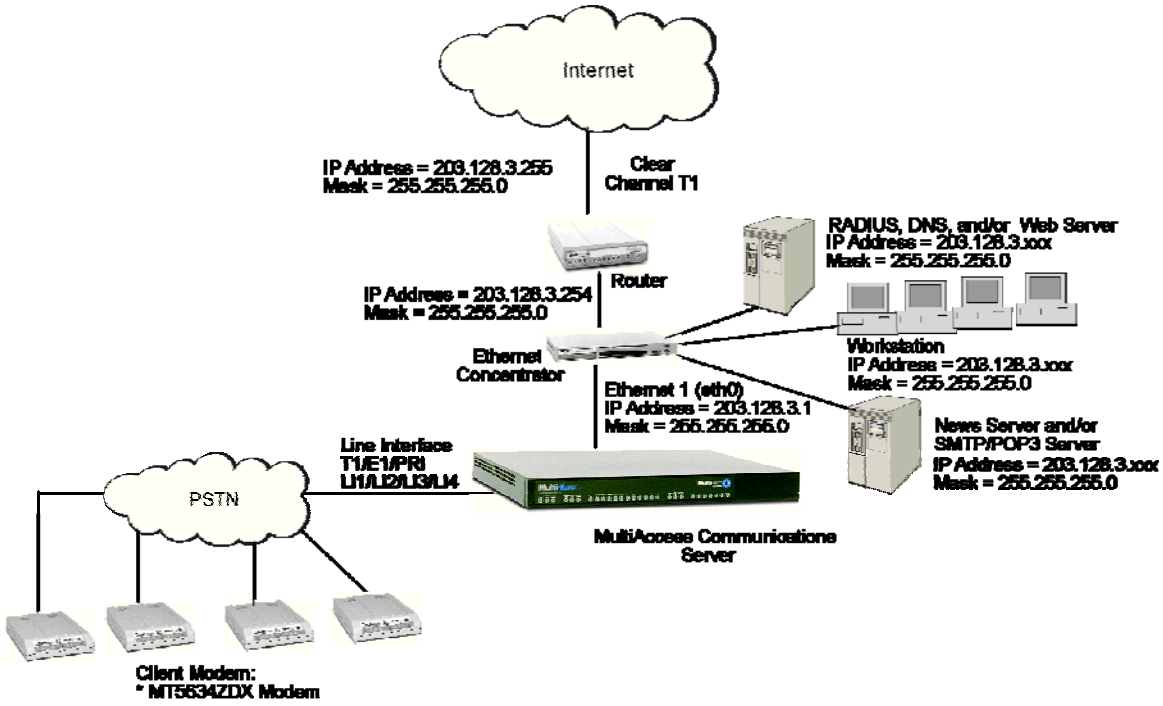


Back panel

The back panel components are described in detail in the Cabling Procedure section in Chapter 2 of this manual.

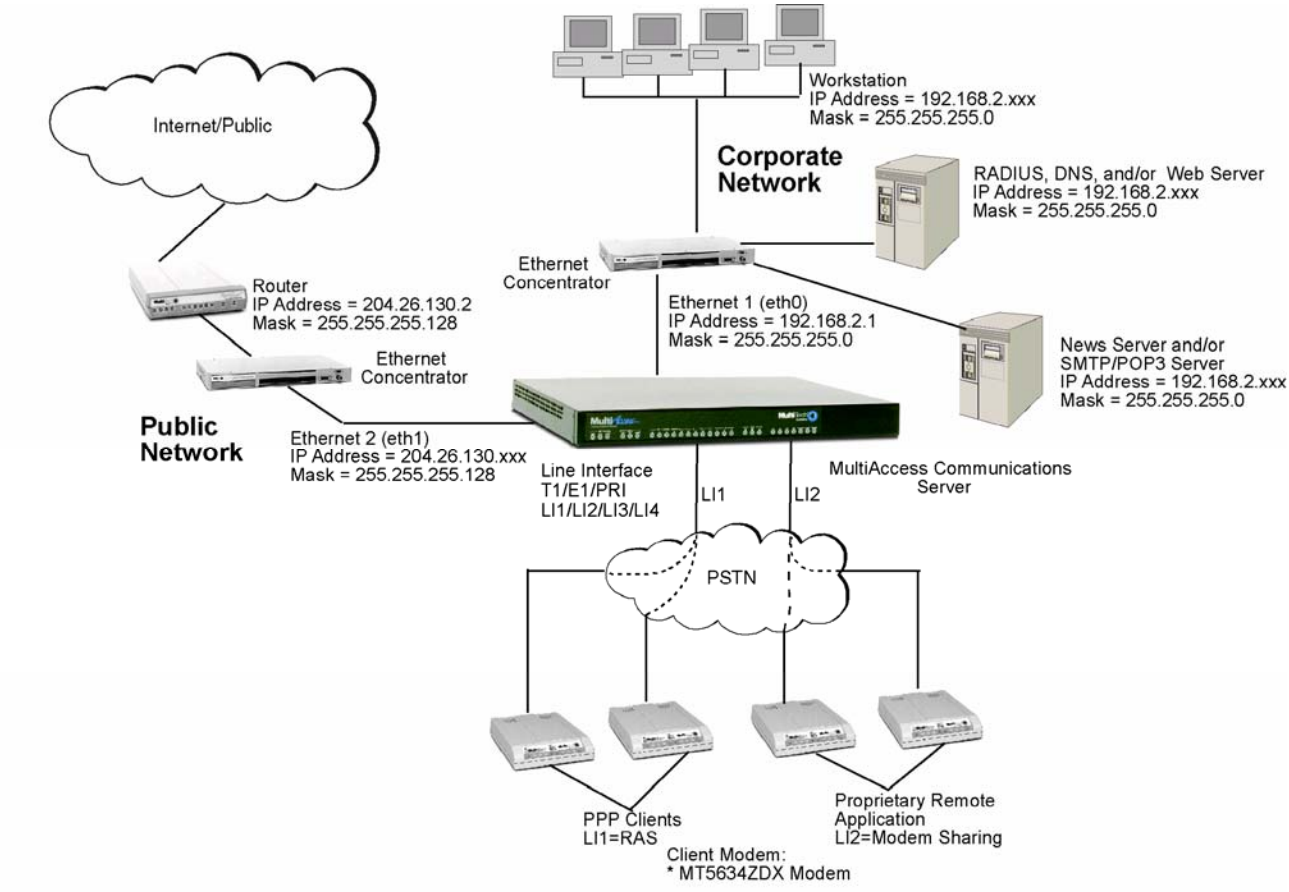
Typical Application

Internet Service Provider (ISP) Application- Only one Ethernet interface on the MultiAccess is used. The IP address of the MultiAccess and the pool of IP addresses for the dial-in users are of the same network and normally are public addresses. The modems of the MultiAccess are configured for RAS usage. PPP clients dial into the system, authenticate, via RADIUS, and establish a LAN to Client PPP session (remote note).



Corporate Application-One or both Ethernet interfaces can be used. When both interfaces are used, they are commonly configured with separate network addresses. The MultiAccess can provide dial-in RAS to one or both networks and provide modem sharing and faxing for network workstations. Workstations on the corporate LAN can be a Comm Port Redirector (e.g., Multi-Tech's WINMCSI) for accessing MultiAccess's modems. Authentication can be performed before granting access to the modem sharing resource, providing another layer of security to your network's infrustructure.

If some or all the MultiAccess's modems are configured for faxing, the HylaFAX™ server software needs to be operating on the MultiAccess and the HylaFAX client software operating on the network workstation.



Specifications

System	Processor: 566 MHz Celeron RAM: 256 MB
LAN Ports	Number of Ports: 2 (LAN 1 and LAN 2 ports) Interface: 2 x 10BaseT/100BaseT (UPT) Format: Ethernet 802.3, 802.2, Ethernet II or SNAP
Server Operating System	Linux Open Source Software
System Management	Web based (HTTPS/SSL)
Security	Port and IP Filtering, Network Address Translation (NAT), Radius support
Modem	Analog Data Rates: V.92/56K, enhanced V.34/33.6K ISDN Data Rates: 64K HDLC, V110 at 19.2K bps & slower Fax Rates: 14.4K bps Error Correction: V.42 Data Compression: V.44, MN5, and V.42bis Fax: V.17, Group 3
ISDN PRI	Channels: 23 (T1 PRI) or 30 (E1 PRI) B-Channel Protocols: PPP, ML-PPP, V.110 Switch Types: NI2, 4ESS, 5ESS custom, DMS100, ETSI, VN6, NTT T1 Frame Formats: Extended Super Frame (ESF), 12 Frame Multiframe (F12), 4 Frame Multiframe (F4), & 72 Frame Multiframe – Remote Switch Mode (F72) T1 Line Code: AMI or B8ZS E1 Frame Formats: Extended Super Frame (ESF) w/ CRC4, Extended Super Frame (ESF) w/o CRC4 (Double Fame) E1 Line Code: AMI or HDB3
Channelized T1	Channels: 24 DSU/CSU operation for T1 WAN service Frame Format: Extended Super Frame (ESF), 12 Frame Multiframe (F12), 4 Frame Multiframe (F4), & 72 Frame Multiframe – Remote Switch Mode (F72) Line Code: AMI or B8ZS Signaling Methods: E&M Immediate, E&M Wink, FXS ground start, FXS loop start
Power	Voltage & Frequency:100-240v AC, 50-60 Hz,1.2-0.6 amps universal input Power Consumption: 30 Watts
Physical Description	17" w × 1.75" h × 10.5" d; 10 lbs. (1U rackmountable) (43.18 cm × 4.45 cm × 26.67 cm; 4.54 kg)
Operating Environment	Temperature Range: 0° to 50° C (32° to 120° F) Humidity: relative 25-85% noncondensing
Approvals	CE Mark EMC: FCC Part 15 Class A, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3 Safety: UL 60950, EN 60950 Telecom: CS03, FCC Part 68, TBR4

Chapter 2 - Installation

Safety Warnings

- Use this product only with UL- and CUL-listed computers.
- To reduce the risk of fire, use only 26 AWG or larger telephone wiring.
- Never install telephone wiring during a lightning storm.
- Never install a telephone jack in a wet location unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone during an electrical storm; there is a risk of electrical shock from lightning.
- Do not use a telephone in the vicinity of a gas leak.

Caution: Danger of explosion if battery is incorrectly replaced. A lithium battery on the MultiAccess board provides backup power for the time-keeping capability. The battery has an estimated life expectancy of ten years. Contact Multi-Tech if you suspect a failed battery. If date and time is incorrect after having the unit powered off, it may be due to a weak battery or incorrect setup.

Caution: The Ethernet ports are not designed to be connected to a Public Telecommunication Network.

Safety Recommendations for Rack Installations

- Ensure proper installation of the MultiAccess in a closed or multi-unit enclosure by following the recommended installation as defined by the enclosure manufacturer. Do not place the MultiAccess directly on top of other equipment or place other equipment directly on top of the MultiAccess.
- If installing the MultiAccess in a closed or multi-unit enclosure, ensure adequate airflow within the rack so that the maximum recommended ambient temperature is not exceeded.
- Ensure that the MultiAccess is properly connected to earth ground via a grounded power cord. If a power strip is used, ensure that the power strip provides adequate grounding of the attached apparatus.
- Ensure that the main supply circuit is capable of handling the load of the MultiAccess. Refer to the power label on the equipment for load requirements.
- Maximum ambient temperature for the MultiAccess is 40 degrees Celsius (104° F).
- Properly qualified service personnel should only install this equipment.
- Connect like circuits. In other words, connect SELV (Secondary Extra Low Voltage) circuits to SELV circuits and TN (Telecommunications Network) circuits to TN circuits.

Site Planning

With proper planning, your MultiAccess system can be installed quickly and in a short time. To implement the suggested planning process, you must:

1. Plan for physical space, environmental, electronic and electrical needs. Identify physical installation site. The environment should be properly ventilated with controlled temperature and humidity.

   • Good AC power source with proper Earth Ground.
   • EIA 19" rack, MultiComTower, or standalone installation.
   • Determine where the termination point is for each T1, PRI, or E1 line.
   • Determine physical access point to the Ethernet network.
   • Identify high quality category 5 cable for Ethernet & T1 cabling. Depending on environment characteristics, shielded T1 cable may be necessary.
   • For initial setup and administrative purposes, a network workstation with a WEB browser supporting HTTPS will be needed.

2. Define your users' client computer needs

   • Determine the number of dial in analog modem users
   • Identify client workstation OS (PC running Windows®98/XP/2000, or MAC OS10)
   • Identify client modem types (V.34, V.90, V.92)
   • Identify dial up security protocol (CHAP & PAP)
   • Third-Party Security Devices (SecurID)
   • Identify the Security Database (i.e. user file in RADIUS server or Microsoft SAM\Active directory with IAS) and make sure users have dial in rights with framed protocol PPP attribute

3. Identify applicable network resources (IP address of; gateway/default route, DNS, WINS, RADIUS server(s), etc)

   • Identify the network MASK
   • Identify available IP addresses (determine the static IP address that is to be assigned to the Multi Access)
   • Determine IP assignment method (predefined pool/range) to be implemented by the MultiAccess (regarding the IP addresses to be assigned to the remote dial in users).
   • When Implementing RADIUS Authentication and Accounting, identify the UDP ports used by the RADIUS server(s)

4. Define your line interfaces

   • Obtain T1 or E1 PRI line provisioning information for your LEC
   • Identify the telephone number(s) of the line or lines
   • Identify the Framing Format
   • Identify the Line Coding
   • Identify the type of signaling (RBS or PRI for T1 or E1 PRI)
   • For RBS, the signaling type can be referred to as the start method and/or the FXS signaling method (i.e. Immediate, Wink, Ground, and Loop)
   • For PRI signaling identify the type of central office switch\protocol, i.e. AT&T5ESS, DMS100/250, National ISDN2
   • Identify the Line Build-Out (LBO) i.e. what db level is presented on premise by the provider and what db level should the premise equipment transmit at.

   Note: For E1 lines the signaling type must be PRI. R2 signaling methods are not supported.

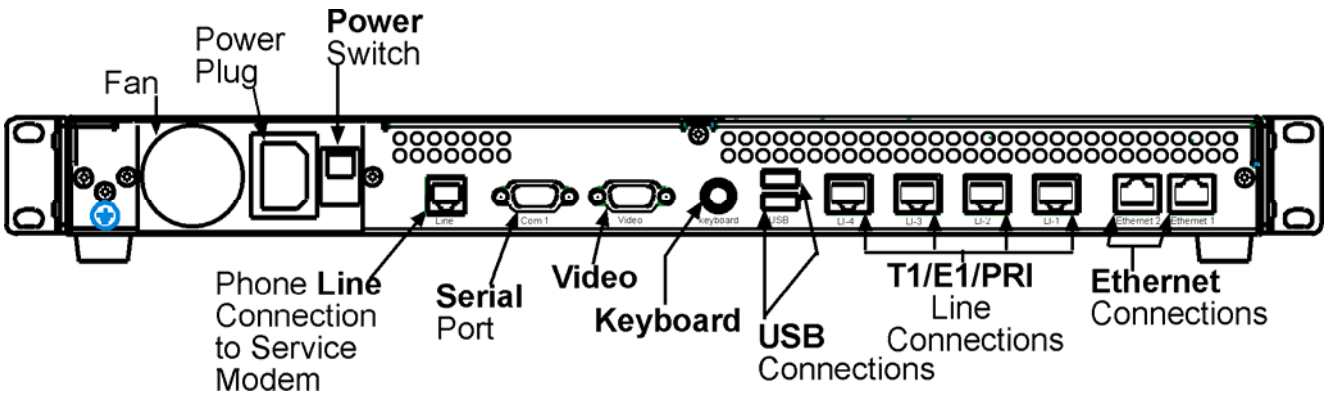
Hardware Installation Procedure

The MultiAccess is designed to install either on a desktop or in a standard EIA 19“ rack, and is shipped with the mounting hardware to install the MultiAccess in the rack. If installing in a rack, use the provided mounting hardware and follow the rack enclosure manufacturer’s instructions to safely and securely mount the MultiAccess in the rack enclosure. Proceed to the cabling procedure.

Cabling

Cabling your MultiAccess involves making the proper power, phone, and line (T1/E1/PRI) connections as described and illustrated below.

The MultiAccess back panel has a fan, a power plug, **POWER** Switch (**| / O**), a RJ-11 phone **LINE** jack, a DB-9 **COM1** jack, a DB-15 High-density DSUB (**VIDEO**) jack, two **USB** (Revision 1.1 compliant) jacks, four RJ-45 **T1/E1/PRI** line jacks, and two **Ethernet** RJ-45 (Ethernet 1 & Ethernet 2) jacks.



1. Using an RJ-45 cable, connect one end to **LI-1** (Line 1 Interface) on the back of the MultiAccess and the other end to your first T1/E1/PRI line connection. If a second, third, or fourth line connection is required, connect an RJ-45 cable for each of the line connections being used.
2. Connect a workstation to your local network; connect one end of a RJ-45 cable to the **Ethernet 1** jack on the back of the MultiAccess and the other end to the hub on your local network.
3. For advanced users, the **Video** and **Keyboard** connections are for manual intervention of the Operating System.

   The default root level login password is linux (lower case) and the command to change the root level password is “passwd”. The recommended mimimum password length is 8-characters. However, the MultiAccess will accept less than 8-characters.

   The Linux command to properly shut down (halt) the MultiAccess is shutdown –h now. The command to restart is r.
4. With the MultiAccess Power switch in the off (O) position and using the supplied power cord, connect the MultiAccess power plug to a live power outlet.
5. Place the MultiAccess Power switch to the on (|) position to turn on the MultiAccess

Caution: Never switch off MultiAccess Power until after you have performed the **Shutdown** process. Refer to **Administration > System Tools** in Chapter 3 of this User Guide. If the MultiAccess is not properly shut down before switching off Power, the next start may take a little longer, or in the worst case, data could be lost.

6. Proceed to Starting the MultiAccess.

Starting Your MultiAccess

This section covers the steps for connecting a workstation to the MultiAccess, starting up the MultiAccess, opening the MultiAccess Communications Server Web Management program, performing the time zone setup, and using the menu bar to navigate through the Web Management software screens.

1. Set the workstation IP address to **192.168.2.x** subnet other than 192.168.2.1 which is the IP address of Ethernet 1 (eth0) and 192.168.2.5 which is already assigned to Ethernet 2 (eht1).
2. Turn on power to the MultiAccess. When you hear 5 beeps, approximately 2 minutes after applying power, continue with the next step.

   Note: Depending on the version of MultiAccess (and other variables, like the previous shutdown and the number of expansion modules) the duration needed to boot may vary. It may be helpful to connect an external monitor and keyboard to determine the current status of the system. Five seconds after turning on power, one beep is heard, indicating a successful POST of the mother board, next the BIOS detects the hard drive from which the Linux operating system and appropriate drivers are loaded.
3. Bring up a Web browser on the workstation. At the browser's address line, enter **https://192.168.2.1** and press the **Enter** key.

   Important: Be sure to type **https** (http will not work).
4. In some environments, one or more Security Alert screen(s) may display. At the initial **Security Alert** screen, click **Yes** and follow any additional on-screen prompts.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate matches the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

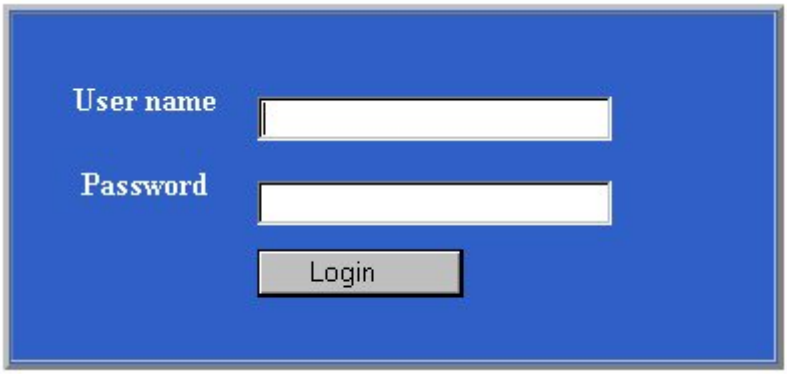
Login

1. The **Login** screen is displayed.
   - Type the default User name: **admin** (all lower-case)
   - Tab to the Password entry and type the default password: **admin** (all lower-case).
   - Click the **Login** button.

   Note: User name and **Password** are case-sensitive (both must be all lower-case) and can be up to 12 characters each. Later, you will want to change the password from the default (**admin**) to something else. (If Windows displays the **AutoComplete** screen, for security reasons, you may want to click **No** to tell Windows OS to not remember the password.)

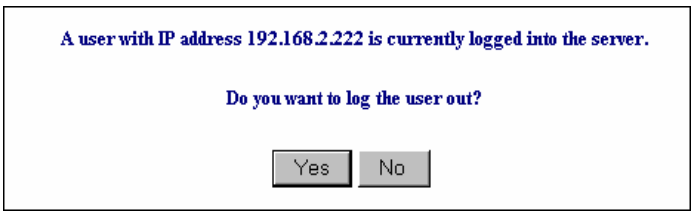
Changing the Password: You should change the default User and Password entries. This can be accomplished in the WEB Admin screen of the Administration menu.

Caution: Use a safe password! Your first name spelled backwards is not a sufficiently safe password; a password such as xfT35$4 is better.



2. If someone else is already logged onto the MultiAccess or you were logged in recently, the following message displays.

At the prompt **Do you want to log the user out?** Click **Yes**. If you click **No**, you are returned to the Login screen.



3. The MultiAccess™ Communications Server Web Management **Home** screen is displayed.

MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
MultiAccess™ Communications Server Version 1.14
2205 Woodale Drive
Mounds View, MN 55112
United States
TEL: (763) 785-3500 or (800) 328-9717
FAX: (763) 785-9874
Tech Support: (800) 972-2439
Web Site: www.multitech.com
FTP Site: ftp.multitech.com
Tech Support:tsupport@multitech.com
MultiAccess
Done
Internet

Navigating Through the Screens

When you click one of the MultiAccess Menu Bar buttons, the first screen for that function displays. Once the first screen opens, you can navigate to other screens within this function; they are listed on the left side of the screen.

Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help

Home: The main screen.
Administration: System setup such as Time & Date, Web management, and certificate. Provides for system shutdown and restart, plus other administrative tools such as PING, Trace Route, and TCP Connect.
Networks & Services: Define networks, services, and groups to make them available to be used by other functions such as allowed networks, and packet filters.
Network Setup: Set up the LAN 1, and LAN 2 Ethernet ports, etc.
DHCP Server: Configure the DHCP server settings.
System Update: Update services can be downloaded from the update server to keep your system continually updated.
Logout: Logout and return to the login screen
Tracking: Set up tracking of all packets through the network ports in the MultiAccess.
Packet Filters: Define filter rules and ICMP rules.
User Authentication: Defines security protocol methods, passwords, and user database details.
Modem Setup: Defines the primary role of the modem; RAS, fax, or network modem pool.
Statistics & Logs: View and download all the statistics and log files maintained by your system.
Line Interfaces: Defines setup information of your PSTN lines.
Help: (Online Help) Describes what to do on each screen.

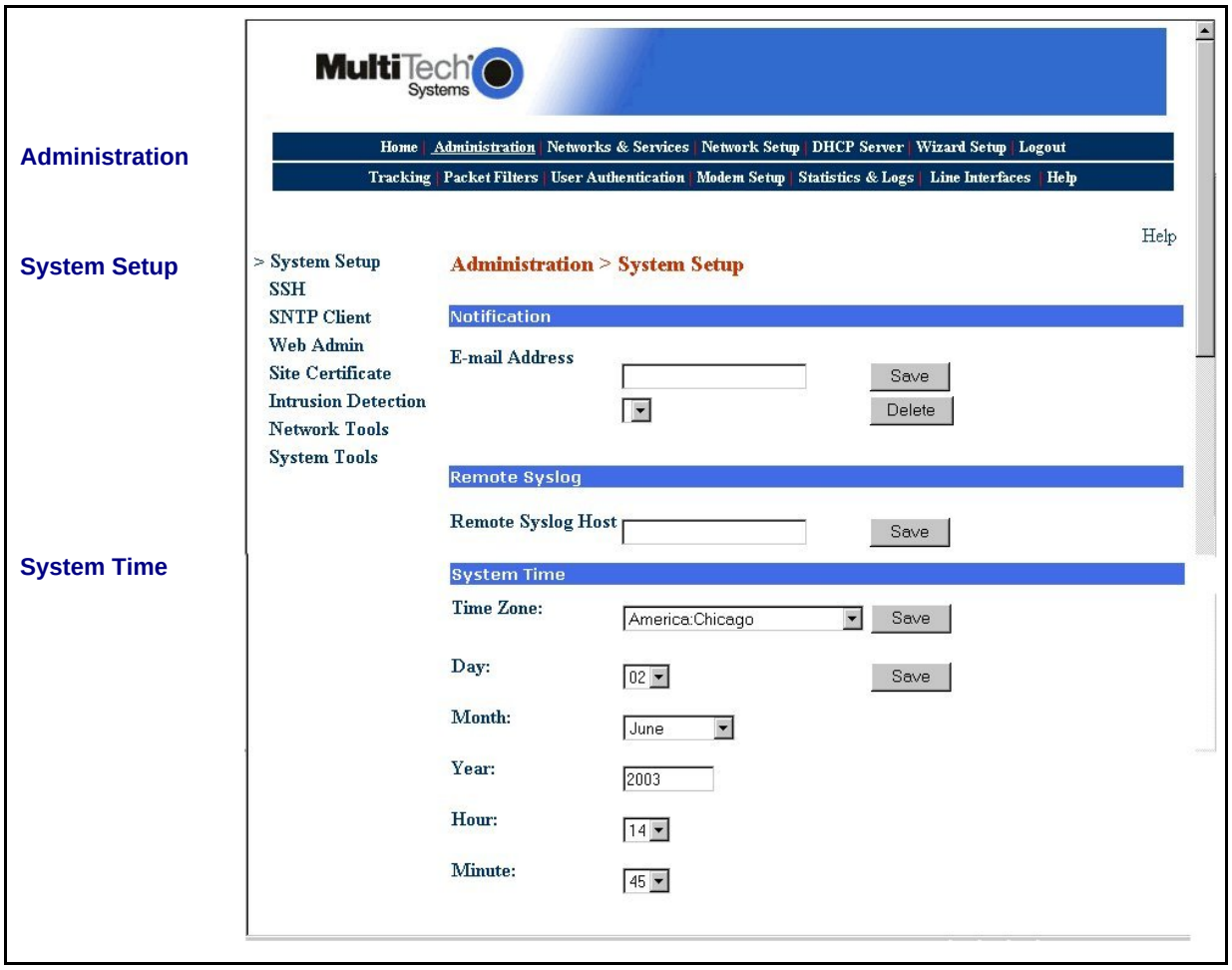
Options Under Each Menu

Home	Administration	Networks & Services	Network Setup	DHCP Server	System Update	Logout
Return to the Main Menu	System Setup SSH SNTP Client Web Admin Site Certificate Database Setup Backup Setup Available Backups Intrusion Detection Network Tools System Tools	Networks Services Network Groups Service Groups	Interface Routes Masquerading SNAT DNAT	Subnet Settings Fixed Addresses	Available Applied Setup	Exit the Program
Tracking	**Packet Filters**	**User Authentication**	**Modem Setup**	**Statistics & Logs**	**Line Interfaces**	**Help**
Accounting	Packet Filter Rules Add User Defined Filters ICMP	Local Users Radius Client Radius Server	Modem Setup Modem Usage Fax Setup	Setup Uptime Networks Interface Details, Routing Table, Network Connections Line Interfaces Status Modem Connections Connections, connection Details, Caller ID, Call History Server Connections Interface Accounting Self Monitor View Logs	Line 1 Setup Line 2 Setup Line 3 Setup Line 4 Setup	Administration Networks & Services Network Setup DHCP Server System Update Tracking Packet Filters User Authentication Modem Setup Statistics & Logs Line Interfaces

Setup Your Time Zone

4. Click **Administration** on the menu bar. The **System Setup** screen displays.

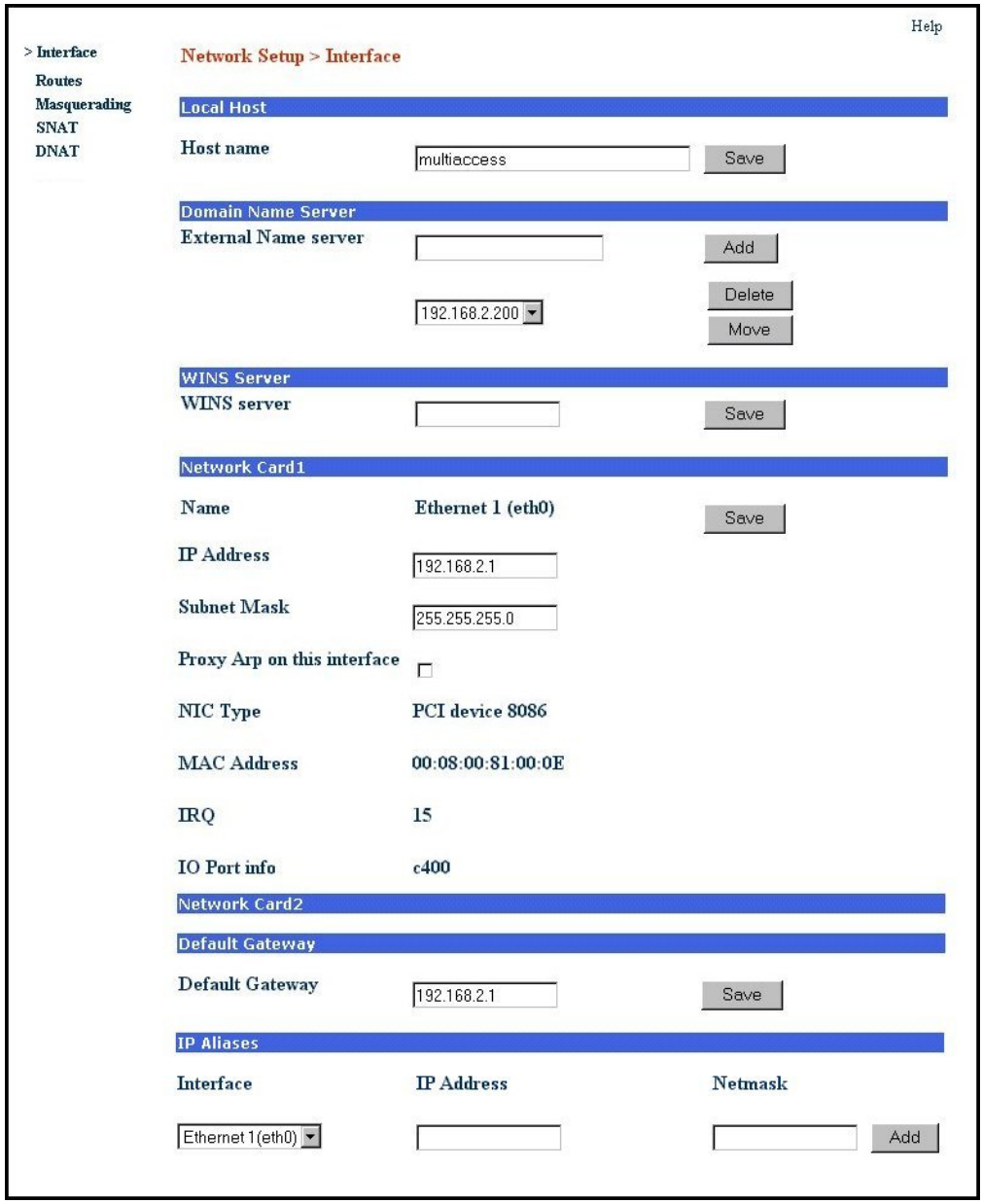
Set the **System Time** by selecting your **Time Zone**, the current **Day**, **Month**, **Year**, **Hour**, and **Minute**.



Network Setup

In the Network Setup > Interface you can define a host name for your MultiAccess, change the Ethernet 1 (eth0) to your local IP and subnet mask for your local network, and change the IP address of the default Gateway to your local gateway address.

1. Enter the **Host name** you have established for your local MultiAccess. Click **Save**.
2. Enter in the **External Name server** window the IP address of your domain name server (DNS).
3. Click the **Add** button to connect to your name server.
4. Change the default **IP Address** for the Network Card 1 to the IP address of your local network and change the default **Subnet Mask** for the Network Card 1 to the subnet mask for your local network. Click **Save**.
5. Change your web browser address to the new address of your local network.
6. Change the **Default Gateway** IP address to the IP address of your gateway. Click **Save**.



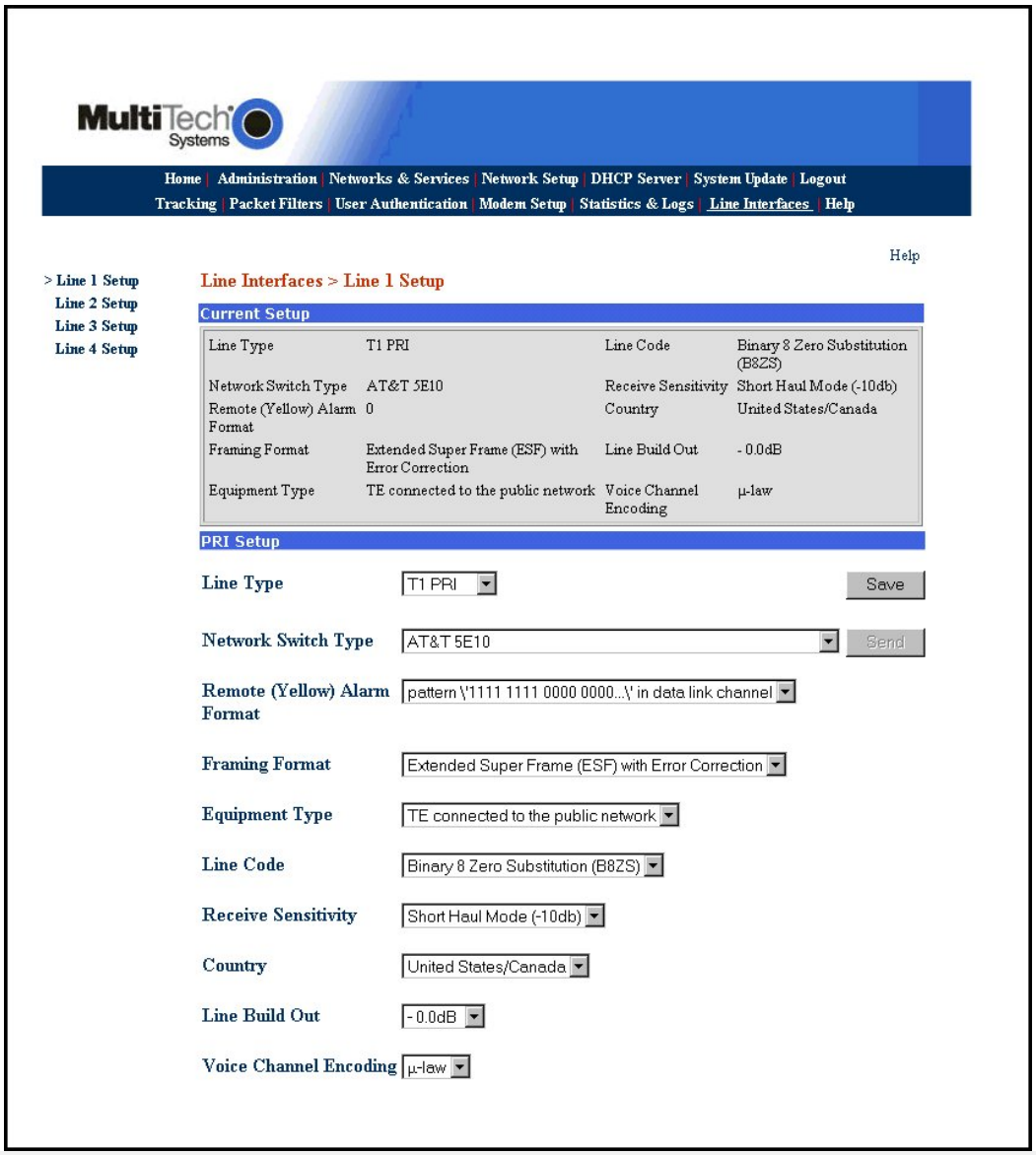
Note: The options for Network Card 2 are not shown in the above screen due to space limitation. The options are the same as for Network Card 1.

Line Interfaces

To establish your line interfaces for the four LI1 through LI4 interfaces, click on **Line Interfaces**. The **Current Setup** section reflects the current operating parameters for the indicated Line Interface.

1. Click on the **Line Type** down arrow and select your type of line interface; T1 RBS or T1 PRI for North America or E1 PRI for the rest of the world, then wait for the screen to refresh.
2. Use the various pull down menus to match the parameters of the Line Interface with the line provisioning information from your Telco.

   Note: A common provisioning issue is the type of framing format which the telco usually refers to as ESF. But, the MultiAccess gives you a choice of ESF or ESF with error correction. Multi-Tech recommends that you choose ESF with Error Correction.
3. Click **Save** and the send button will become active.
4. Click the **Send** button to cause the new parameters to become active. You **must wait 45 seconds** for the screen to refresh and the new configuration to apply, then **Current Setup** section is updated.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
> Line 1 Setup
Line 2 Setup
Line 3 Setup
Line 4 Setup
Line Interfaces > Line 1 Setup
Current Setup
Line Type T1 PRI
Line Code Binary 8 Zero Substitution (B8ZS)
Network Switch Type AT&T 5E10
Receive Sensitivity Short Haul Mode (-10db)
Remote (Yellow) Alarm Format 0
Country United States/Canada
Framing Format Extended Super Frame (ESF) with Error Correction
Line Build Out - 0.0dB
Equipment Type TE connected to the public network
Voice Channel Encoding µ-law
PRI Setup
Line Type T1 PRI
Save
Network Switch Type AT&T 5E10
Send
Remote (Yellow) Alarm Format pattern \'1111 1111 0000 0000...\' in data link channel
Framing Format Extended Super Frame (ESF) with Error Correction
Equipment Type TE connected to the public network
Line Code Binary 8 Zero Substitution (B8ZS)
Receive Sensitivity Short Haul Mode (-10db)
Country United States/Canada
Line Build Out - 0.0dB
Voice Channel Encoding µ-law

Modem Setup

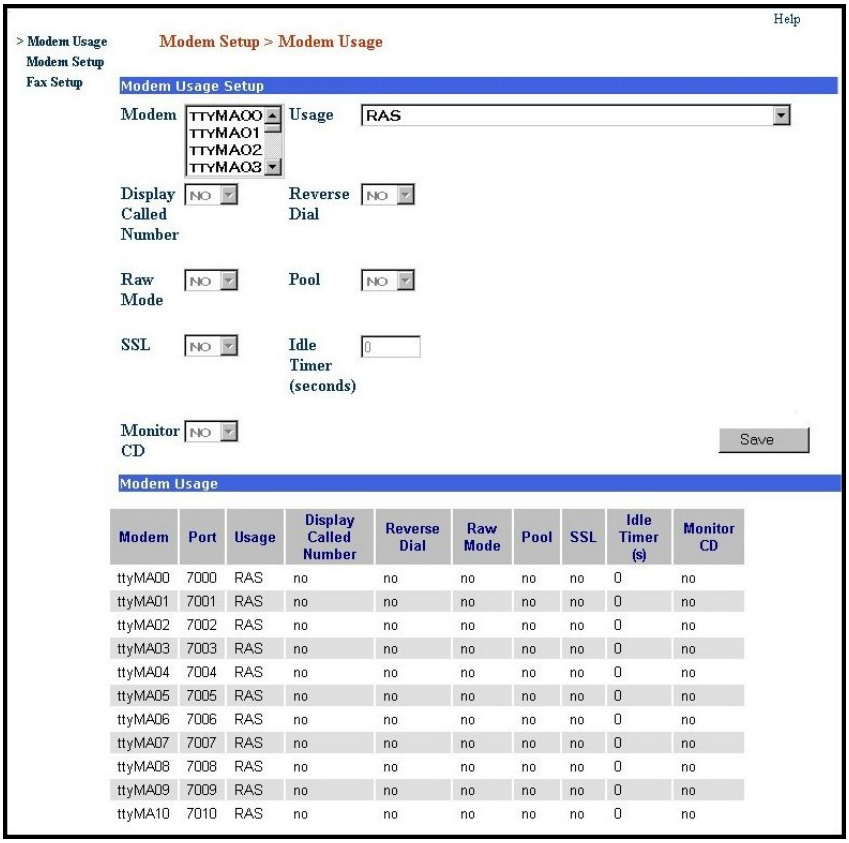
The Modem Setup group of menus configure the modems for usage with RAS, modem sharing, and faxing. The default usage for each modem is RAS. The Modem Setup menu controls the parameters of the modems set to RAS. If the MultiAccess modems are to be used for dialout, in a networking modem sharing environment, then use the Modem Usage menu to change the usage to Modem Sharing. If the MultiAccess modems are to be used for faxing with the integrated Hylafax™ Server, then use the Modem Usage menu to change the usage to Fax. The Fax Setup menu is used to configure the Hylafax Server for sending and receiving faxes.

Note: The MultiAccess modems also support faxing with fax servers that are external to the MultiAccess via the Modem Sharing usage.

Modem Usage

If you are using all your MultiAccess modems to provide dial-in PPP access, you do not have to modify the default Modem Usage settings. The default usage is RAS. If you plan to use all or part of your MultiAccess modems for dial-out, you will have to change the Modem usage settings for the selected modems to one of the Modem Sharing options that best fit your needs. If you plan to use some or all your modems for faxing, you will have to change the Modem Usage setting for the selected modems to Fax.

If you are using your MultiAccess in an RAS inbound PPP environment, you do not have to make any changes in the Modem Usage menu.

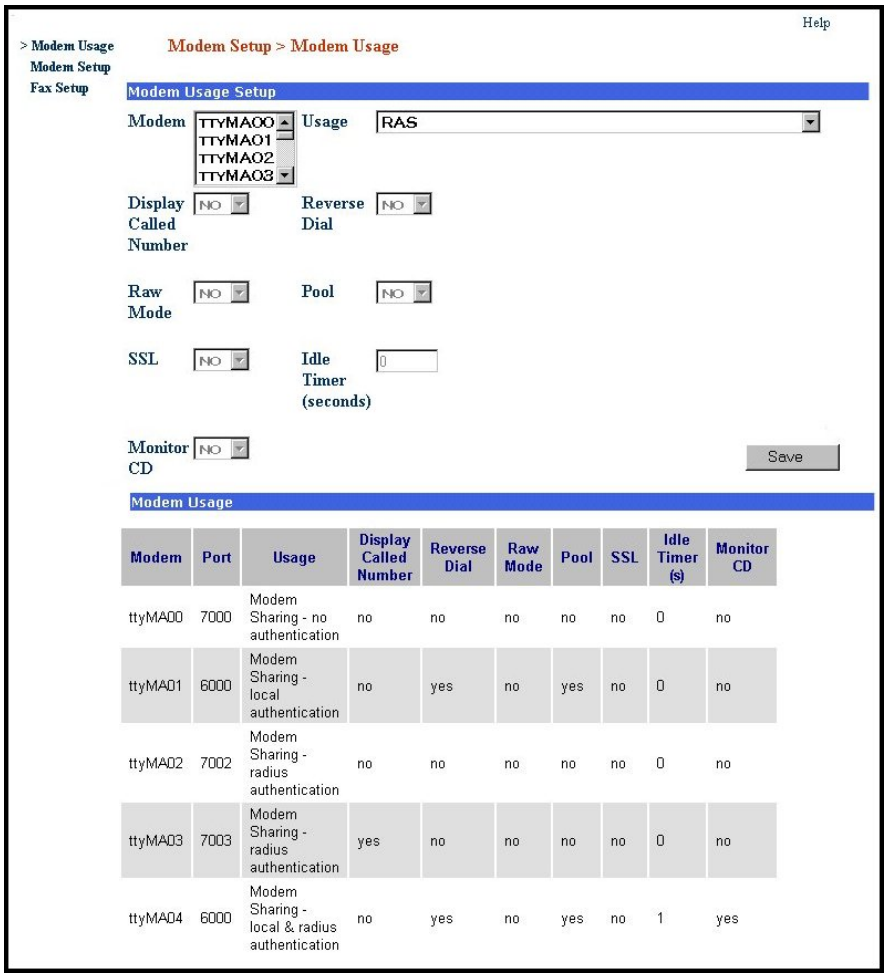


Modem	Port	Usage	Display Called Number	Reverse Dial	Raw Mode	Pool	SSL	Idle Timer (s)	Monitor CD
ttyMA00	7000	RAS	no	no	no	no	no	0	no
ttyMA01	7001	RAS	no	no	no	no	no	0	no
ttyMA02	7002	RAS	no	no	no	no	no	0	no
ttyMA03	7003	RAS	no	no	no	no	no	0	no
ttyMA04	7004	RAS	no	no	no	no	no	0	no
ttyMA05	7005	RAS	no	no	no	no	no	0	no
ttyMA06	7006	RAS	no	no	no	no	no	0	no
ttyMA07	7007	RAS	no	no	no	no	no	0	no
ttyMA08	7008	RAS	no	no	no	no	no	0	no
ttyMA09	7009	RAS	no	no	no	no	no	0	no
ttyMA10	7010	RAS	no	no	no	no	no	0	no

Note: When implementing a combination of usage options, care must be given so that inbound calls do not conflict with outbound calls. This may require changing the hunt group call distribution at the central office and should be addressed with the provider of your T1/E1 digital line.

Caution: Modem sharing is accomplished by implementing a Telnet interface to the MultiAccess modems. Make sure that care is taken to secure access to these ports via firewall or IP filter settings to prevent unauthorized use of your modem resources.

If you are using your MultiAccess as a network modem pool, you will need to set up the Modem Usage menu to support your configuration.



Modem	Port	Usage	Display Called Number	Reverse Dial	Raw Mode	Pool	SSL	Idle Timer (s)	Monitor CD
ttyMA00	7000	Modem Sharing - no authentication	no	no	no	no	no	0	no
ttyMA01	6000	Modem Sharing - local authentication	no	yes	no	yes	no	0	no
ttyMA02	7002	Modem Sharing - radius authentication	no	no	no	no	no	0	no
ttyMA03	7003	Modem Sharing - radius authentication	yes	no	no	no	no	0	no
ttyMA04	6000	Modem Sharing - local & radius authentication	no	yes	no	yes	no	1	yes

1. Click on the **Usage** drop down arrow and chose the Modem Sharing – authentication type that suits your applicational needs.
2. Click on the **Modem** drop up or down arrow and select the tty modem(s) for modem sharing. You can choose multiple modems by holding down the shift key.
3. When the Modem Usage is set to Modem Sharing, the following options become available:

   Display Called Number - This parameter applies to inbound (received) calls when the Line Interface type is PRI. The telephone number (or final digits) dialed by the originator will be displayed into the telnet socket following the first “ring” message. The Called Number information (string of digits) is provided by the central office switch and is commonly referred to as DNIS. The MultiAccess does not support DNIS when the Line Interface type is T1-RBS.

   Reverse Dial - This parameter enables two features, comma dialing and reverse dial mode. When enabled, the dial string can include the use of commas, used to create a pause between digits of the dial string (most commonly used to specify the extension of the answering modem).

   Example: “atdt18003334444,,,,,4321”. Each comma creates a 2 second pause. 4321 is the extension of the desitination phone line\modem.

   Reverse dial mode is where the dial string includes the letter “r” at the very end of the dial string, the purpose of which is to instruct the MultiAccess modem to switch from originate to answer mode after dialing. For example: “atdt17637175549r”.

   Please Note: When Reverse Dial is enabled, the dial string must include the tone (t) command, for example, atd**t***string* .

Raw Mode - If **Yes**, this sets the TCP port to a RAW socket. User data is treated “as is” and the Telnet Command Escape capability is disabled. If **No**, this allows the Telnet command parser to look for escape sequences that are used to communicate control functions. A common example is to support RFC-2217 Com Port Control.

Pool - If you want to access a specific modem, accept the default of No. Each modem will be given a specific TCP port number, starting at 7000+. If you select pool = Yes, then all selected modems are accessed via port number 6000 – creating a first available pool, starting with the lowest numbered tty port.

SSL - Support is made available when the usage is **Modem Sharing** with **Authentication**. This is only used with SSL capable Telnet Clients. Site Certificate information needs to be configured appropriately. Contact Multi-Tech Tech Support for additional information.

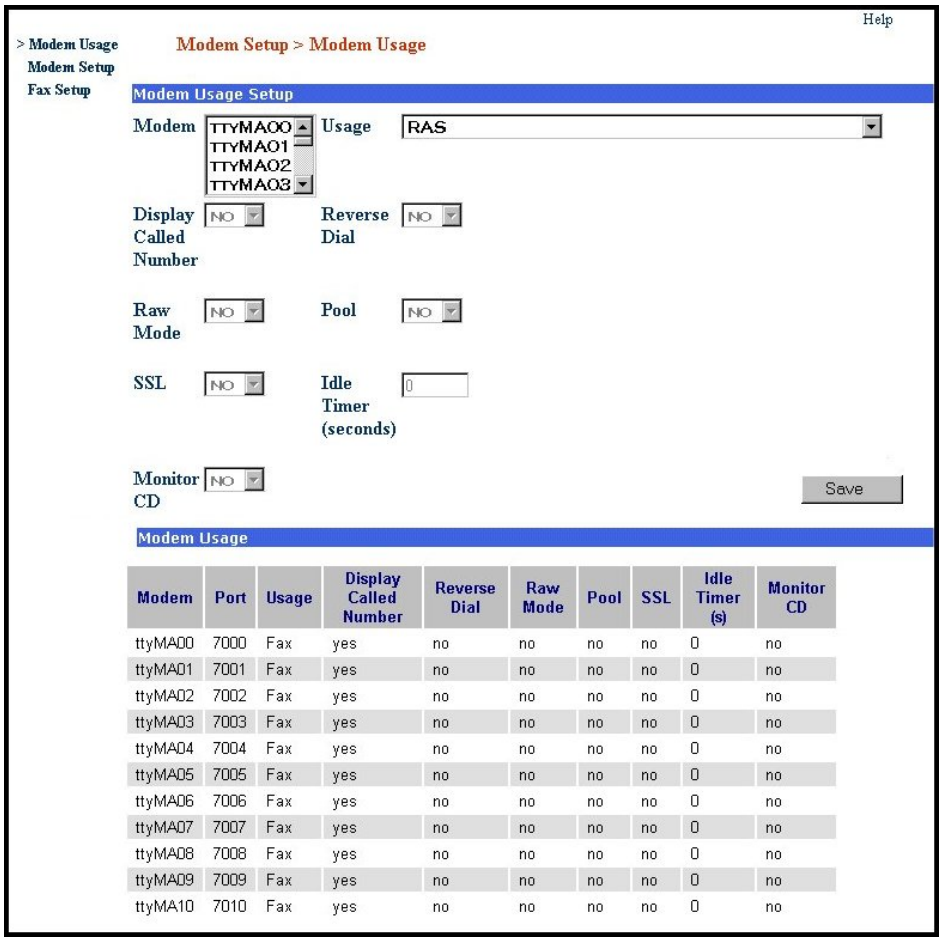
Idle Timer (seconds) - The Idle Timer, upon expiring, will hangup the modem and close the telnet socket. Idle time is defined as no data flow in both directions. Any data sent or received across the socket will cause the Idle Timer to start over. When there has been no data activity for the duration specified, the idle timer will expire.

Monitor CD - Upon the modem disconnecting, the MultiAccess will close the telnet socket to the host application server.

4. Click on the **Save** button.

If you are using your MultiAccess as a network fax server, you need to set up the Modem Usage menu to support your configuration.

5. Click on the **Usage** drop down arrow and select Fax.
6. Click on the **Modem** up or down arrow and select the tty modem(s) for faxing. You can choose multiple modems by holding down the shift key.
7. Click on the **Save** button.

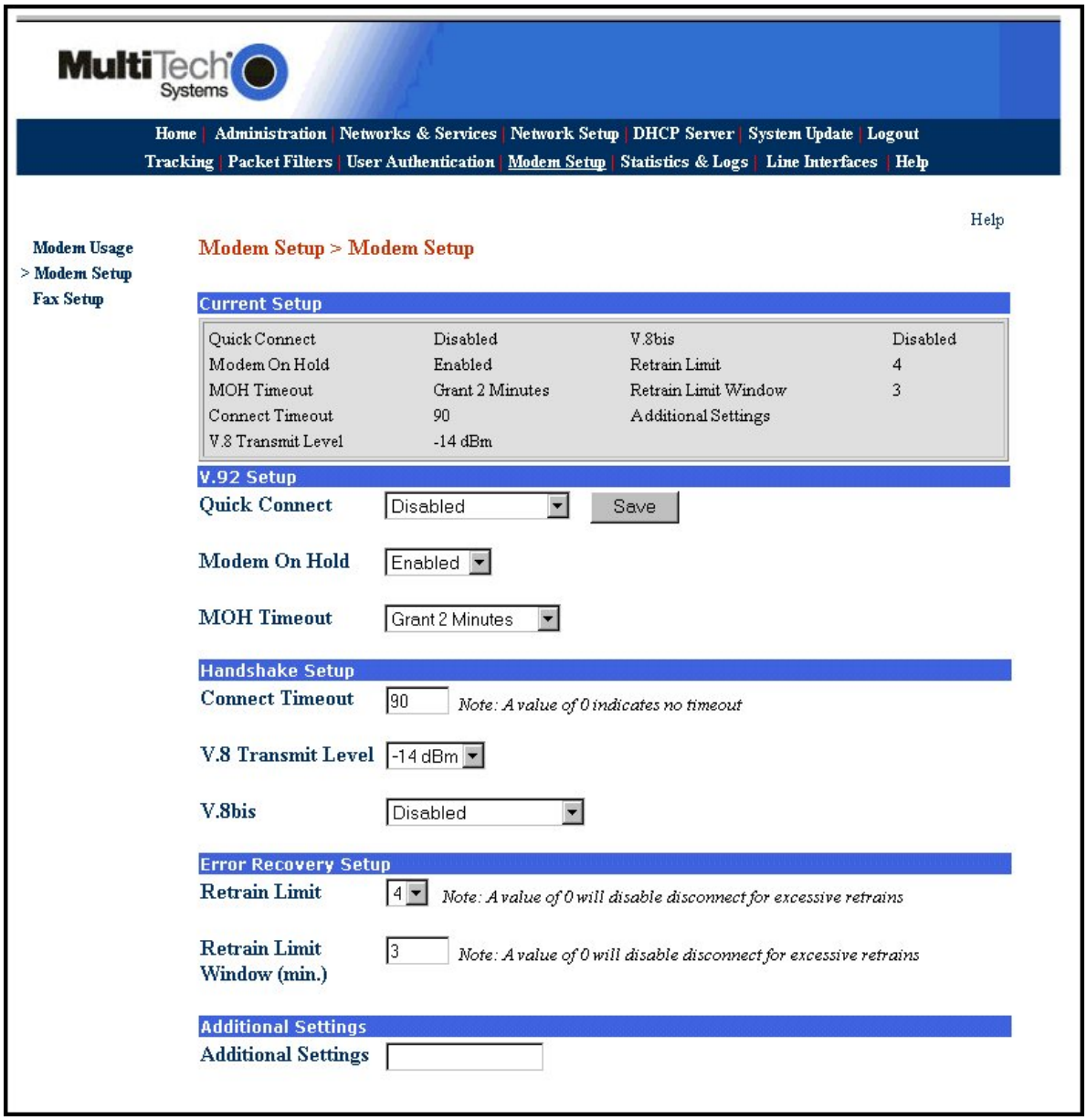


Modem	Port	Usage	Display Called Number	Reverse Dial	Raw Mode	Pool	SSL	Idle Timer (s)	Monitor CD
ttyMA00	7000	Fax	yes	no	no	no	no	0	no
ttyMA01	7001	Fax	yes	no	no	no	no	0	no
ttyMA02	7002	Fax	yes	no	no	no	no	0	no
ttyMA03	7003	Fax	yes	no	no	no	no	0	no
ttyMA04	7004	Fax	yes	no	no	no	no	0	no
ttyMA05	7005	Fax	yes	no	no	no	no	0	no
ttyMA06	7006	Fax	yes	no	no	no	no	0	no
ttyMA07	7007	Fax	yes	no	no	no	no	0	no
ttyMA08	7008	Fax	yes	no	no	no	no	0	no
ttyMA09	7009	Fax	yes	no	no	no	no	0	no
ttyMA10	7010	Fax	yes	no	no	no	no	0	no

Modem Setup

Modem Setup screen only applies when the Modem Usage is set for RAS (Dial-in PPP). RAS usage is defined in the Modem Usage Setup field of the Modem Usage screen.

1. Verify that the **V.92 Setup** parameters conform to your client's characteristics.
2. Multi-Tech recommends that you set **Retrain Limit** to 4 and due to compatibility issues seen with various modems, you may wish to disable **Quick Connect** and **V.8bis**.
3. If additonal modem commands are required, refer to Appendix B, Advanced Commands.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Modem Usage
> Modem Setup
Fax Setup
Modem Setup > Modem Setup
Current Setup
Quick Connect Disabled V.8bis Disabled
Modem On Hold Enabled Retrain Limit 4
MOH Timeout Grant 2 Minutes Retrain Limit Window 3
Connect Timeout 90 Additional Settings
V.8 Transmit Level -14 dBm
V.92 Setup
Quick Connect Disabled Save
Modem On Hold Enabled
MOH Timeout Grant 2 Minutes
Handshake Setup
Connect Timeout 90 Note: A value of 0 indicates no timeout
V.8 Transmit Level -14 dBm
V.8bis Disabled
Error Recovery Setup
Retrain Limit 4 Note: A value of 0 will disable disconnect for excessive retrains
Retrain Limit Window (min.) 3 Note: A value of 0 will disable disconnect for excessive retrains
Additional Settings
Additional Settings

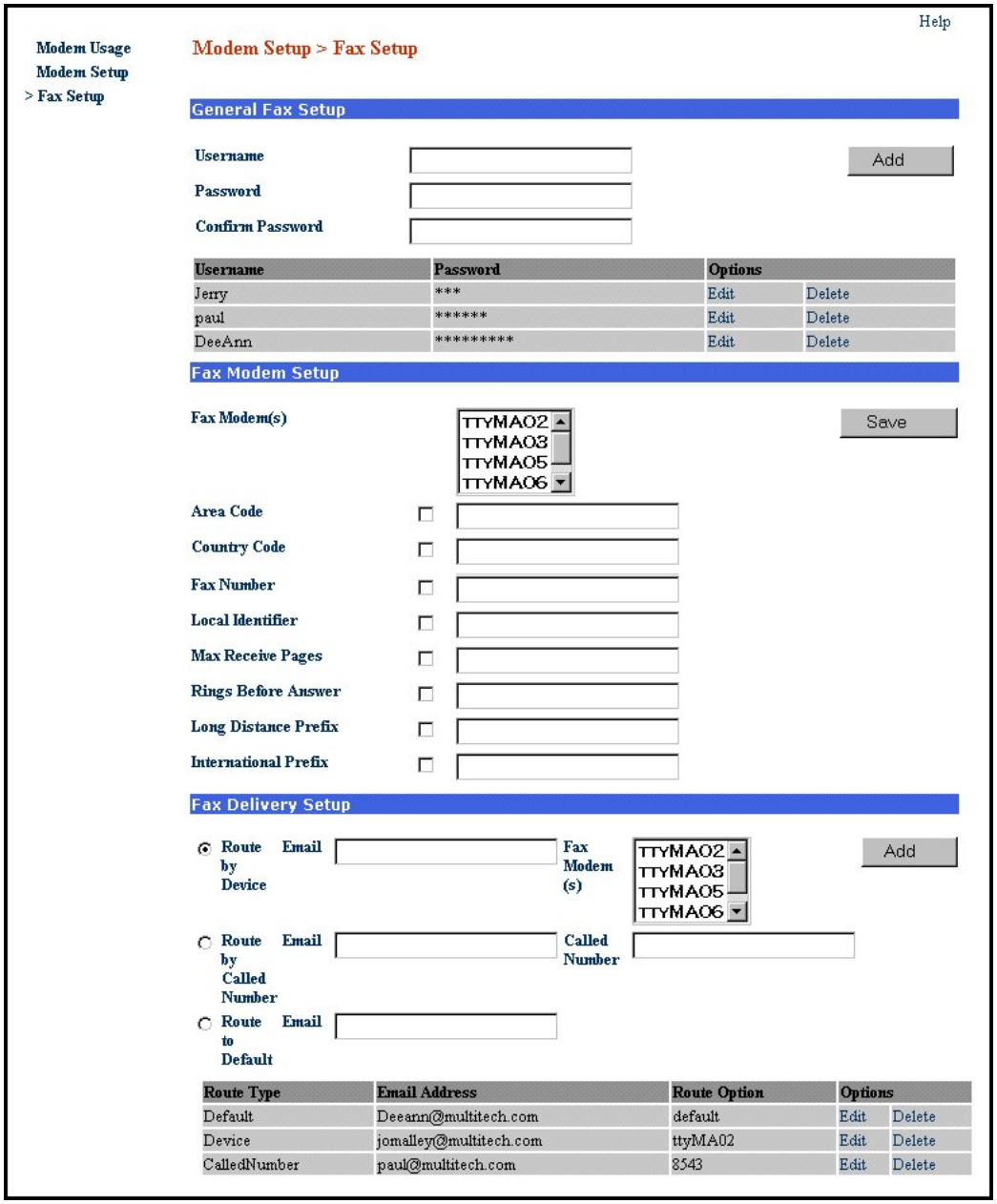
Fax Setup

Fax setup is initiated when you allocate modem(s) to the integrated Hylafax™ Fax Server. This is achieved by setting the selected modem's usage to Fax. If no modems are set for fax usage, then only the General Fax Setup section is displayed. The Fax Setup screen is used to configure the integrated Hlyfax Server for sending and receiving faxes.

The sending of outbound faxes via the Hylafax Server requires the use of a Hylafax compatible Fax Client software, e.g., Multi-Tech's FaxFinder Client. The General Fax Setup group is used to add Fax Clients to the Hylafax server.

The Fax Client must be installed on each workstation that you wish to send faxes from. The Fax Client must use the credentials defined in the General Fax Setup group to submit faxes for sending. The Fax Client is not used for receiving faxes.

Inbound faxes received from the T1/E1 digital line are converted to tiff files and then emailed from the Hylafax server to the specified recepient. The Fax Delivery Setup group is used to configure the routing of inbound faxes.



Outbound Fax Client Data Base

The outbound fax client data base is generated in the General Fax Setup group. The current outbound fax client data base is shown in the table at the bottom of the General Fax Setup group. The credentials defined here are to be used by the fax client. The fax client uses these credentials when accessing the Hylafax server.

1. To establish a fax client data base, enter each **user name** and **password** in their respective windows and click the **Add** button for each entry.

   Note: All fax clients can use the same set of credentials, or a unique set for each client can be added.

Fax Modem Settings

These settings are used to define the fax station identity and other administrative variables. The default settings are normally sufficient with the exception of the "Rings Before Answer" parameter. When the Called Number feature is used, the Rings Before Answer must be set to 2 for all the ports. Each Fax Modem is to be configured with a unique Local Identifier, which is used as the TSI (Transmit Station Identifier) when sending faxes and is included in the body of the email when receiving faxes. You can limit the maximum number of pages being received.

Inbound Fax Data Base

The Fax Delivery Setup group is used to configure the routing of inbound faxes. The current fax routing table is shown at the bottom of this group. Who the fax should be delivered to (routed to) is determined by one of two routing methods:

A) "Route by Device" (what tty port the fax was received on),

B) Route by Called Number" (number dialed by the remote sender).

Route by Device is a static delivery method, where all faxes that are received on that particular port will be sent to the email address defined for that port.

8. To deliver the fax based on the port (device) it was received on, select the radio button "Route by Device" and then highlight the ttyMXxx port(s) from the corresponding window in the Fax Delivery Setup group,

1. Enter the email address of the fax recipient in the Email window and then click add.

Route by Called Number is a dynamic delivery method that requires the use of a PRI line (T1-PRI or E1-PRI line type). Route entries are to match the DNIS information (provided by Telco per call) to an email address. The Telco switch will (via PRI signaling) provide DNIS digits to the MultiAccess at the time of ringing (call setup). How many digits will Telco be providing? The remote originator of the fax may dial 11 digits (1-800-333-4444) but Telco may only provide the last x number of digits (where x is commonly = 4). DNIS digits provided by Telco is a variable to be determined at the time of ordering and installing the PRI service. If no Called Number route entries can be matched to the DNIS provided for that call - the default route entry will be used.

1. To deliver the fax based on the number dialed, select the radio button "Route by Called Number".

2. Enter the email address of the fax recipient in the Email window.

3. Enter the DNIS string matching the number dialed and then click add.

9. The entry should be added to the route table found at the bottom of the screen.

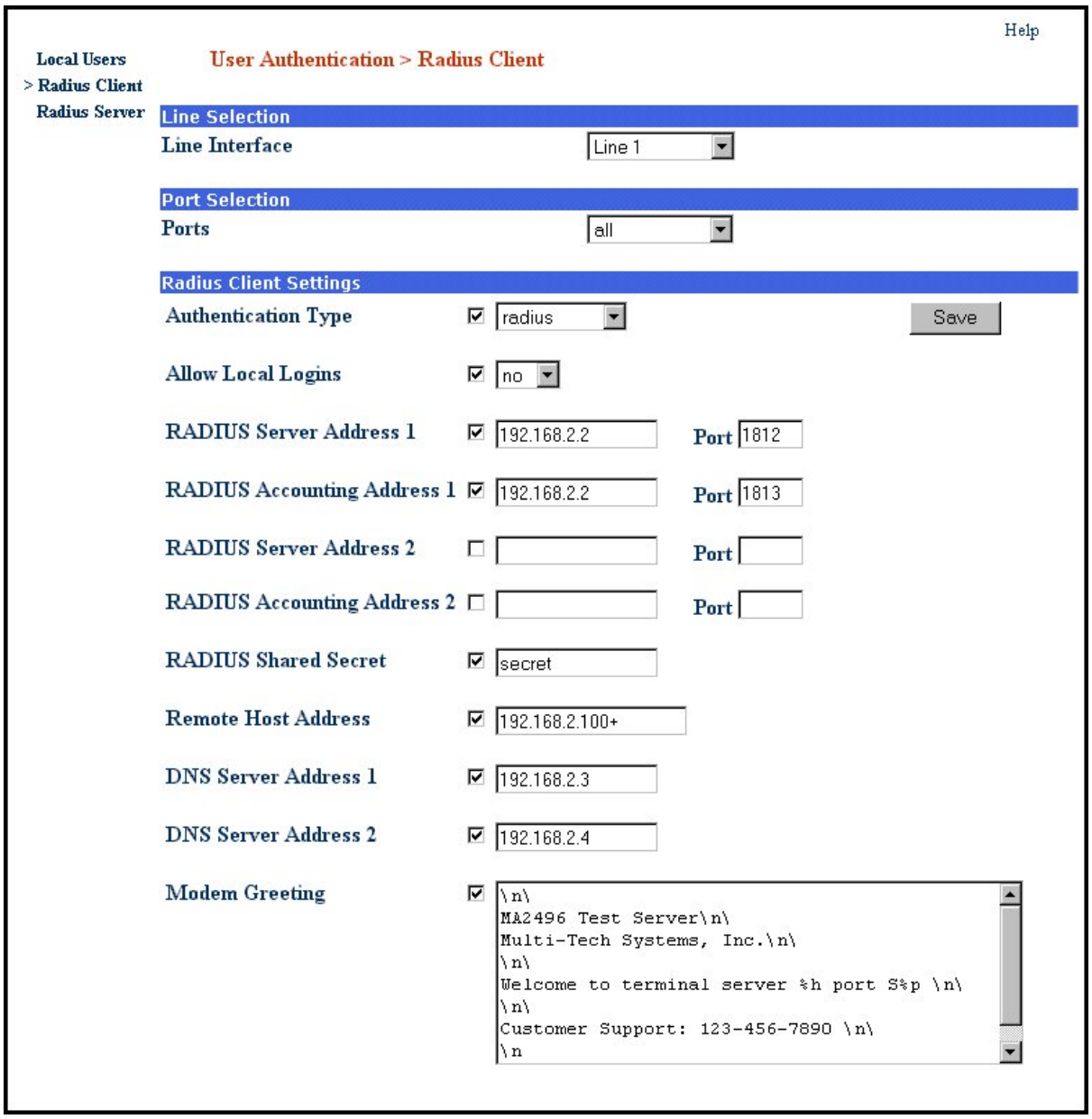
User Authentication

User authentication is established using Radius Client and Radius Server screens. The Radius Client informs the MultiAccess of where the Radius Server is located. If your network already has a Radius Server, you do not have to enter the Radius Server screens. The Radius Server screens are only used when the Radius Server in the MultiAccess is going to be used. Initially the Radius Server > Default User Setup screen displays the default settings that are used for dial in network access. Initially these default settings are all that you should need to authenticate a remote user.

Note: When using the internal Radius Server, you must use the IP address of network card 1 (eth0).

Radius Client

1. Choose **User Authentication >Radius Client**.
2. Click on **Line Interface** and select the Line number you selected in the Line Interface screen.



3. Choose the **Authentication Type** that is being used in your situation by clicking on the down arrow and highlighting the Authentication Type. **Radius** is the default. You can choose from none, radius, tacacs, remote, local, and radius/local.
4. We recommend that you leave Allow Local Logins set to the default of **no**.

   Caution: If you change this to yes and put a "!" before the login name, you could be setting up a potential security risk. You can use this in an **emergency situation** if your radius server goes down.
5. Enter the IP address of your main Radius server in **RADIUS Server Address 1** window.

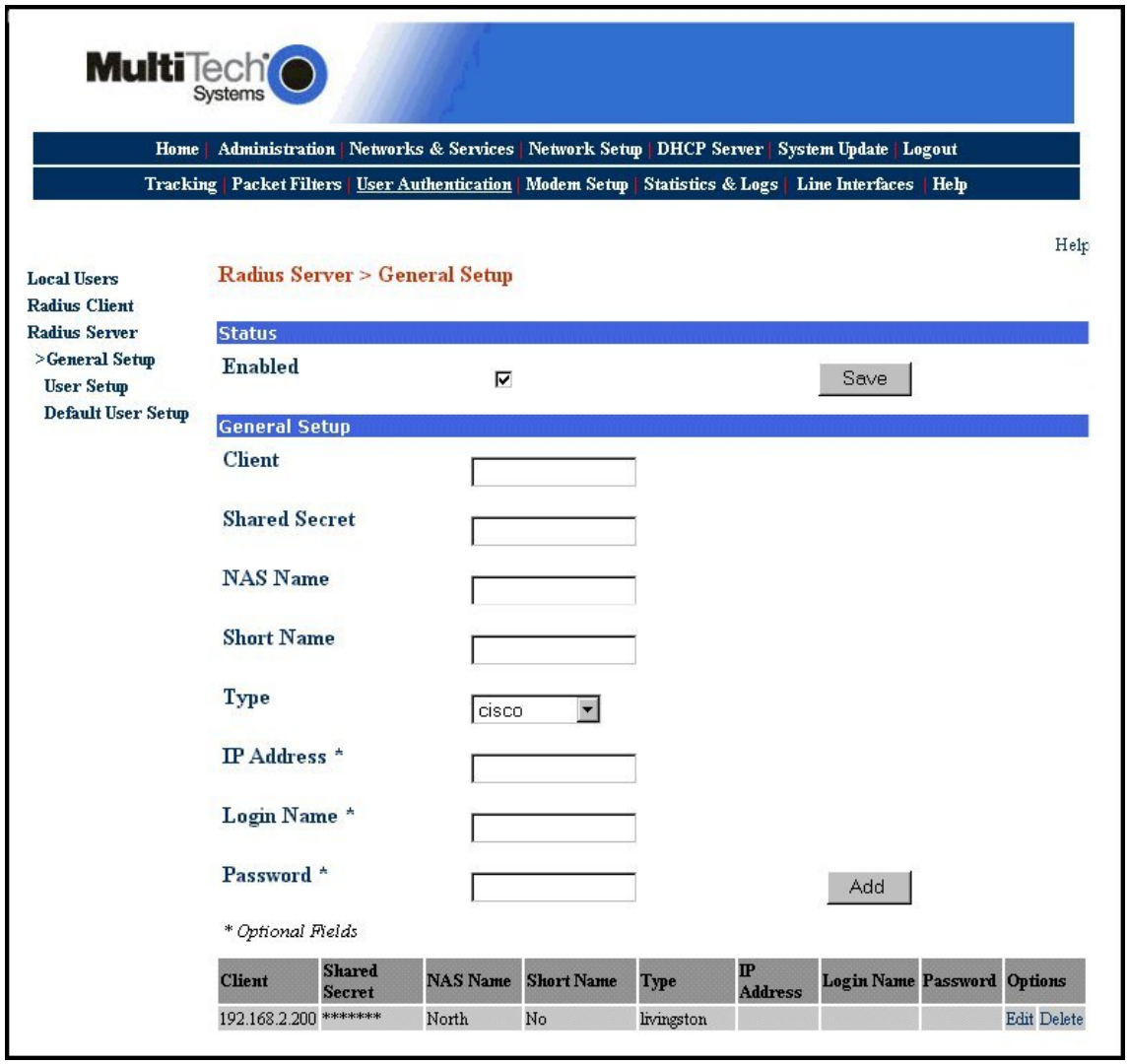
   Note: When using the internal Radius Server, both server and client must used the IP address network card 1 (eht0).
6. Enter the UDP port number used by your main Radius server in the first **Port** window.
7. Enter the IP address of your main Radius Accounting host in the **RADIUS Accounting Address 1** window.
8. Enter the UDP port number used by your main Radius Accounting host in the second **Port** window.
9. If you have a second (backup) Radius server, enter the IP address for the backup Radius server in the **RADIUS Server Address 2** window. Follow that by entering the port number of the backup Radius server in the third **Port** window. Then enter the backup Radius Accounting host in the **RADIUS Accounting Address 2** window followed by the port number for the backup host in the fourth **Port** window.
10. Enter your Shared Secret for the Radius Server in the **RADIUS Shared Secret** window.
11. In the **Remote Host Address** window, set the starting IP address of your IP address pool (addresses that are to be assigned to the dial in users). The IP address needs to have a + (plus symbol) after the number (e.g., 192.168.1.150+). The plus symbol instructs "Portslave" to create an address pool starting with the address you have entered. Portslave determines the "ending" address number by adding up all the Line Interface selections that have their "Port Selection" set to "All". If the MultiAccess server has multiple line interface modules and all ports are to use an address pool, set this field to the same address (192.168.1.150+) for each line interface.
12. Enter the IP address of your primary name server in the **DNS Server Address 1**. This establishes the name server for remote access users. If you have a backup DNS server, enter the IP address of your backup DNS Server in the DNS Server Address 2 window.
13. Click the **Save** button when you are finished.
14. Repeat the above procedure for each line interface.

Radius Server > General Setup

If you are going to use the Radius Server that comes with your MultiAccess, then you need to tell the Radius Server who the Radius Clients are. You need one entry for each Network Access Server (NAS) in your network.

Note: When using the internal Radius Server, you must use the IP address of network card 1 (eth0).

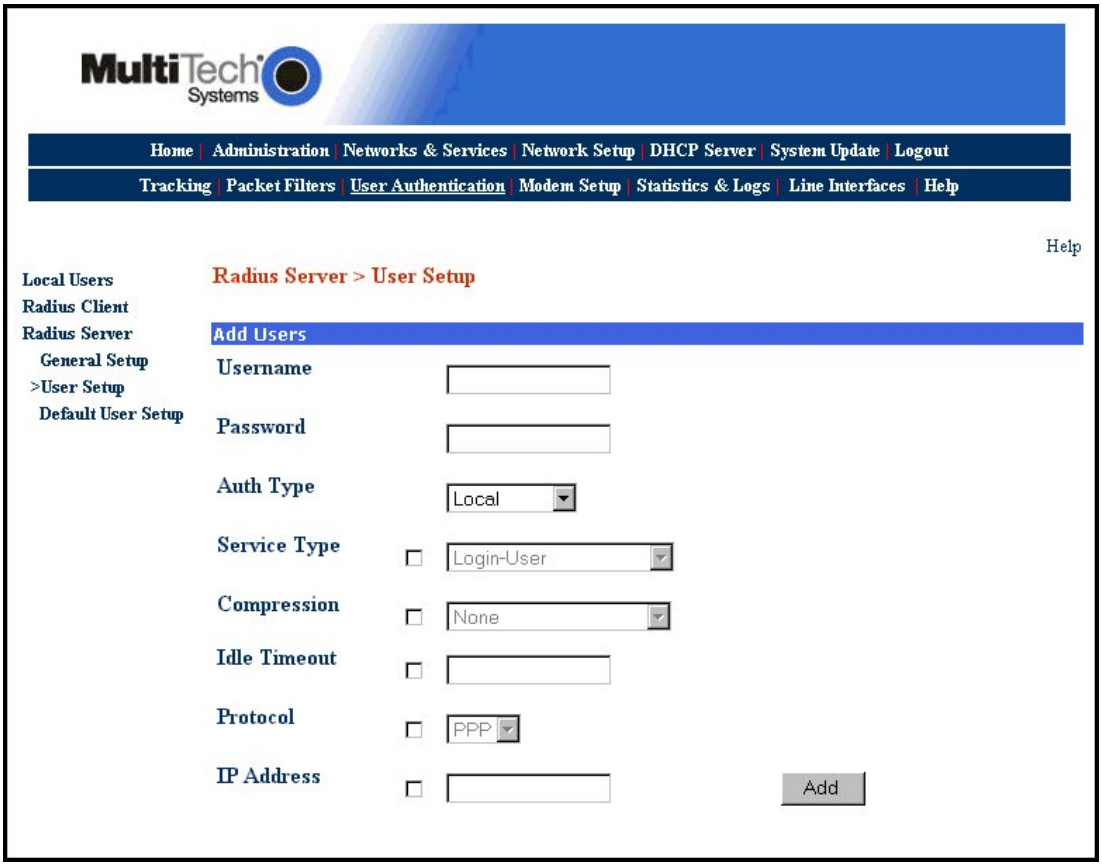
1. You can enable status by clicking on the **Enabled** window.
2. Enter the IP address of network card 1 (eth0) in the **Client** window. This IP address tells the Radius Server where the Radius Client is located.
3. Enter the same Shared Radius Secret used in the Radius Client screen in the **Shared Secret** window. The Shared Secret in the Radius Server and the Radius Server Secret in the Radius Client have to be the same in order for the two to communicate.
4. You can enter an arbitrary name, unique name for each NAS in the **Short Name** window.
5. Select the manufacture of radius client/NAS that is being used in your system from the **Type** drop down arrow. For example, multitech, livingston, or etc.
6. The three optional items are to restrict logins.
7. Click **Add** when you are finished.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Local Users
Radius Client
Radius Server
>General Setup
User Setup
Default User Setup
Radius Server > General Setup
Status
Enabled
Save
General Setup
Client
Shared Secret
NAS Name
Short Name
Type
cisco
IP Address *
Login Name *
Password *
Add
* Optional Fields
Client | Shared Secret | NAS Name | Short Name | Type | IP Address | Login Name | Password | Options
192.168.2.200 | ******* | North | No | livingston | | | | Edit Delete

Radius Server > User Setup

The User Setup screen establishes who the remote access user is. A user name and password has to be entered for each remote user that is dialing in to the MultiAccess. The User name and password of the remote user is all that is needed initially. If you check or enable Service Type through IP Address windows you will over ride the Default User Setup.

1. Enter the remote user's name in the **Username** window.
2. Enter the password of the remote user in the **Password** window.
3. The Authentication Type should remain at the default setting.
4. Click the **Add** button when you are finished.



Chapter 3 - Software

This chapter describes each screen and its function in the MultiAccess™ Communications Server software. The aim of the administrator in setting the options in the software should be to let as little as possible and as much as necessary through the MultiAccess, for both incoming as well as outgoing connections.
The Menu bar provides the organization of this chapter.

Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help

Home: The main screen.
Administration: System setup such as Time & Date, Web management, and certificate. Provides for system shutdown and restart, plus other administrative tools such as PING, Trace Route, and TCP Connect.
Networks & Services: Define networks, services, and groups to make them available to be used by other functions such as allowed networks, and packet filters.
Network Setup: Set up the LAN 1, and LAN 2 Ethernet ports, etc.
DHCP Server: Configure the DHCP server settings.
System Update: Update services can be downloaded from the update server to keep your system continually updated.
Logout: Logout and return to the login screen
Tracking: Set up tracking of all packets through the network ports in the MultiAccess.
Packet Filters: Define filter rules and ICMP rules.
User Authentication: Defines security protocol methods, passwords, and user database details.
Modem Setup: Defines the primary role of the modem; RAS, fax, or network modem pool.
Statistics & Logs: View and download all the statistics and log files maintained by your system.
Line Interfaces: Defines setup information of your PSTN lines.
Help: (Online Help) Describes what to do on each screen.

Options Under Each Menu

Home	Administration	Networks & Services	Network Setup	DHCP Server	System Update	Logout
Return to the Main Menu	System Setup SSH SNTP Client Web Admin Site Certificate Database Setup Backup Setup Available Backups Intrusion Detection Network Tools System Tools	Networks Services Network Groups Service Groups	Interface Routes Masquerading SNAT DNAT	Subnet Settings Fixed Addresses	Available Applied Setup	Exit the Program
Tracking	**Packet Filters**	**User Authentication**	**Modem Setup**	**Statistics & Logs**	**Line Interfaces**	**Help**
Accounting	Packet Filter Rules Add User Defined Filters ICMP	Local Users Radius Client Radius Server	Modem Setup Modem Usage Fax Setup	Setup Uptime Networks Interface Details, Routing Table, Network Connections Line Interface Status Modem Connections Connections, Connection Details, Caller ID, Call History Server Connections Interfaces Accounting Self Monitor View Logs	Line 1 Setup Line 2 Setup Line 3 Setup Line 4 Setup	Administration Networks & Services Network Setup DHCP Server System Setup Tracking Packet Filters User Authentication Modem Setup Statistics & Logs Line Interfaces

Home and Logout Options

Home

This is the opening screen of the MultiAccess™ Communication Server Web Management software.

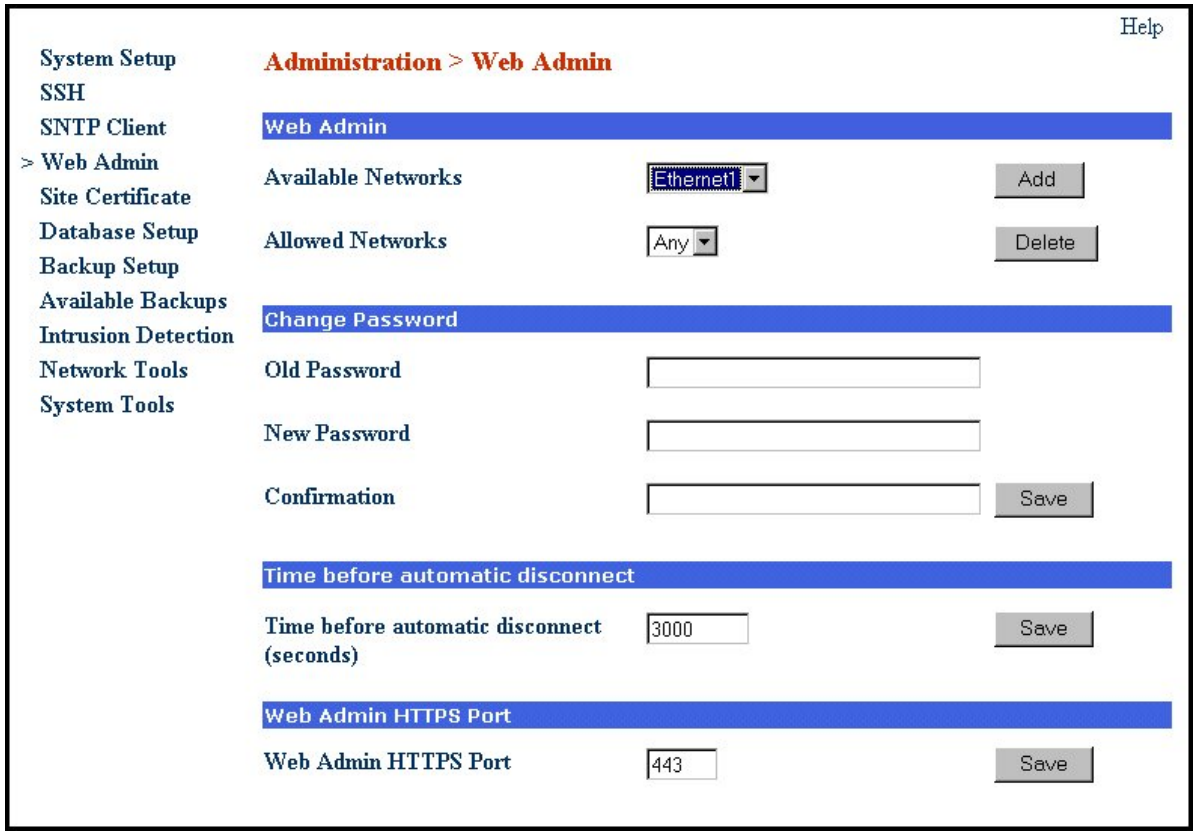
MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
MultiAccess™ Communications Server Version 1.14
2205 Woodale Drive
Mounds View, MN 55112
United States
TEL: (763) 785-3500 or (800) 328-9717
FAX: (763) 785-9874
Tech Support: (800) 972-2439
Web Site: www.multitech.com
FTP Site: ftp.multitech.com
Tech Support:tsupport@multitech.com
MultiAccess
Done
Internet

Logout - How to Exit MultiAccess Communications Server Software

The best way to exit the MultiAccess Communications Server system is to choose **Logout** from the Menu bar.

If you close the browser in the middle of a session without logging out, the session stays active until the end of the time-out. If you reopen the session during the time-out, a prompt comes out saying “Some body is already logged in – Do you want to log the user out?” you respond with Yes and a new session is started. The timeout period is set at **Administration > Web Admin > Time before automatic disconnect**. If you change the **Time before automatic disconnect**, you have to click the **Save** button for the new disconnect time to be active.

When you are done in **Administration > Web Admin**, click **Logout** on the menu bar**.** The browser connection is terminated and you are returned to the **Login** screen. Note that hitting the browser’s **Back** button will not effectively return you to the previous menu or directory.

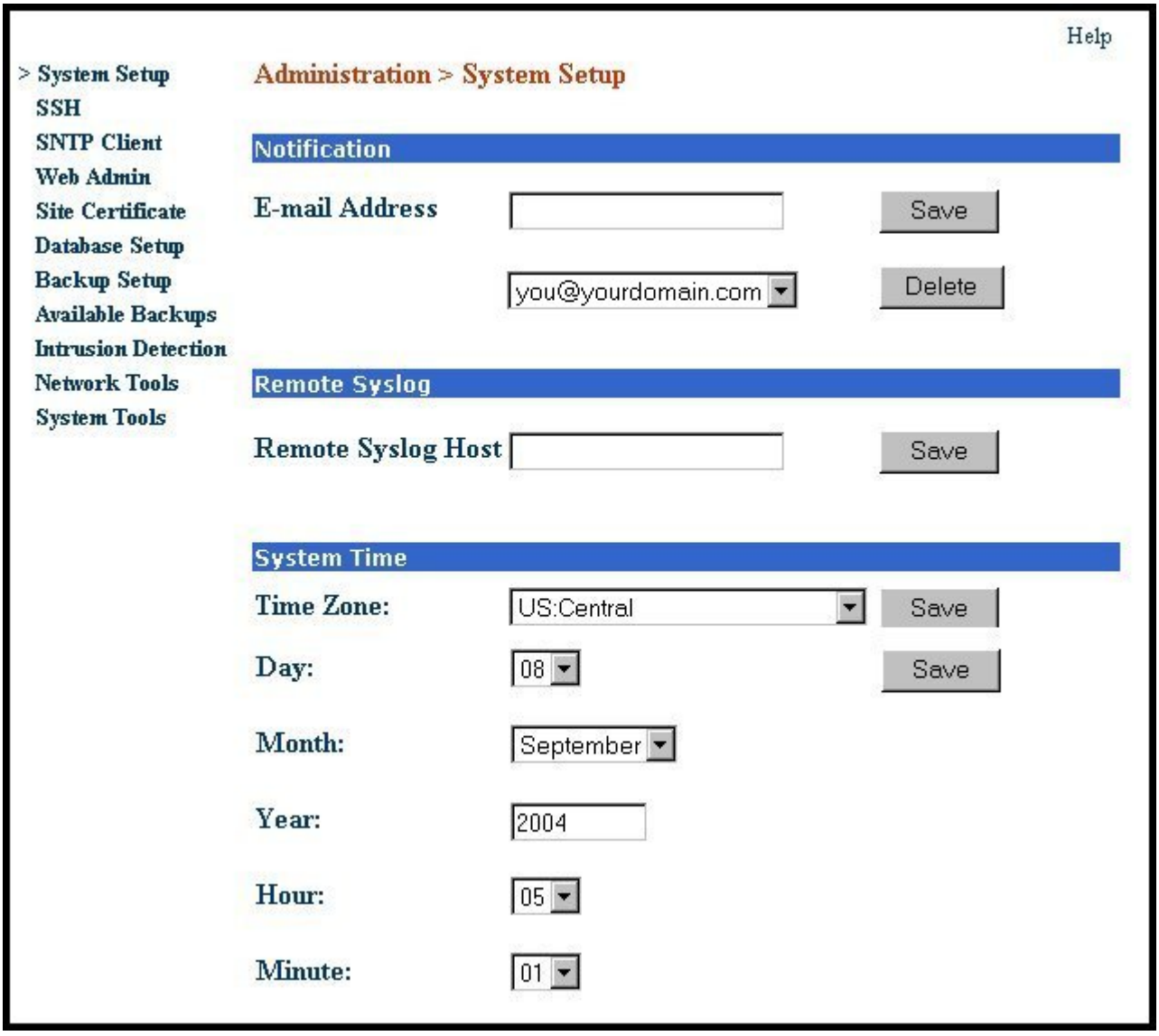


Administration

Administration > System Setup

In the Administration section, you can perform the general system-based settings for the MultiAccess Communications Server functions.

System Setup includes general system parameters such as the email address of the administrator, remote syslog host, and the system time can be set through these settings.



Notification - Email Address

This field defines the email address of the administrator to whom emails must be sent in case of any particular event. The email address has to be entered in proper user@domain format. Emails will be sent to the administrator on hard disk usage exceeding 70%, Intrusion Detections, backups, license key expire, self monitor problems, invalid web logins, and invalid SSH logins. The mail settings have to be saved in the server's configuration. So the session will be terminated and the web server will be restarted.

Type the **Email Address** of the administrator who will receive email notifications of any one of the system events listed below. Click **Save**. You then have the option to delete the entry.

Types of Notifications the MultiAccess Will Send:

- System license key - on expire, from 10 days before expire.
- SSH invalid login - Not
- Web invalid login - Works
- Intrusion Detection - File System Integrity
- Intrusion Detection - SNORT (Network Intrusion Detection)
- Backup - backup file on export will be sent.
- Update services - system update completion.
- Disk usage exceeding 70%, disk usage exceeding 80% (after cleanup)
- Self monitor

Remote Syslog - Remote Syslog Host

In the Remote Syslog field, type the **IP Address** of the desired remote Syslog Host and click **Save**.

This setting enables the sending of all logged messages to a host that is your syslog host.

System Time

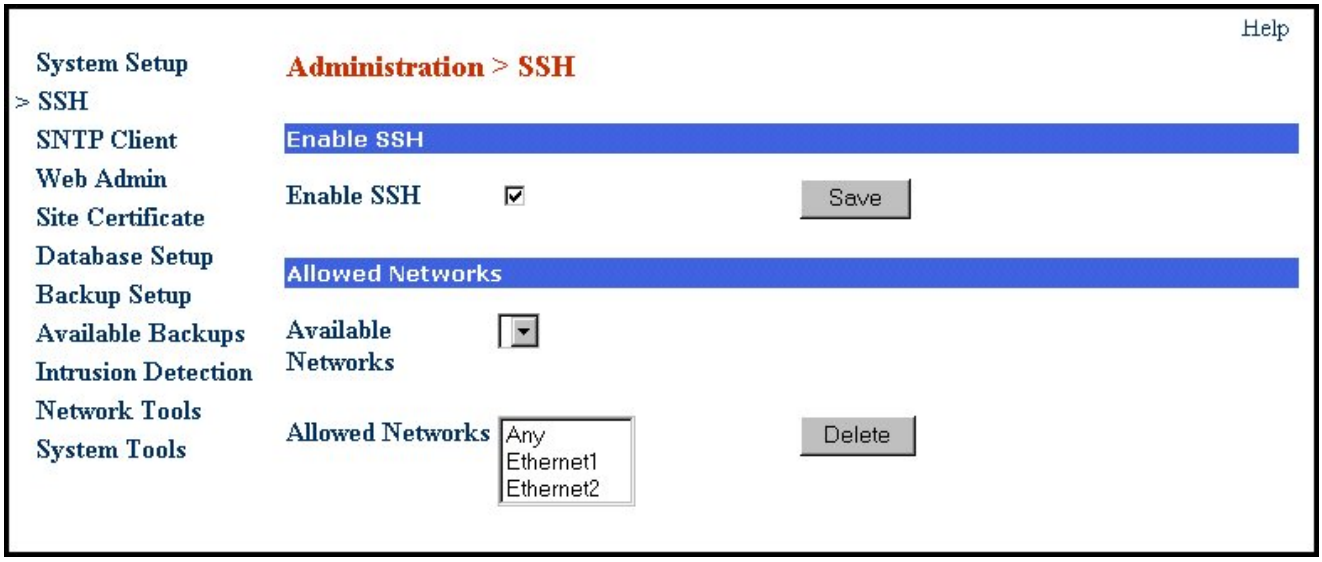
This selection sets the system time. The year, month, hour, and minute have to be selected from the options provided. After the selection is made, click Save to get the system time changed. The selected date should match the corresponding month and year, i.e., if the date selected is 29, month is February and the year is 2001, the time will not be saved because for the year 2001, February has 28 days.

Administration > SSH

SSH (Secure Shell) is a program to log into another computer over a network to execute commands in a remote machine and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is intended as a replacement for rlogin, rsh, and rcp.

SSH is a command line interface. Access via SSH is encrypted.

For access via SSH**,** you need SSH Client, which most Linux systems already include. For MS Windows, the program **PuTTY** is very common as a SSH client.



Status

This screen opens with **Status** as the only prompt. Once it is checked and saved, SSH is enabled and the other options display.

SSH requires name resolution for the access protocol, otherwise a time-out occurs with the SSH registration. This time-out takes about one minute. During this time it seems as if the connection is frozen, or can't be established. After that the connection returns to normal without any further delay.

Allowed Networks

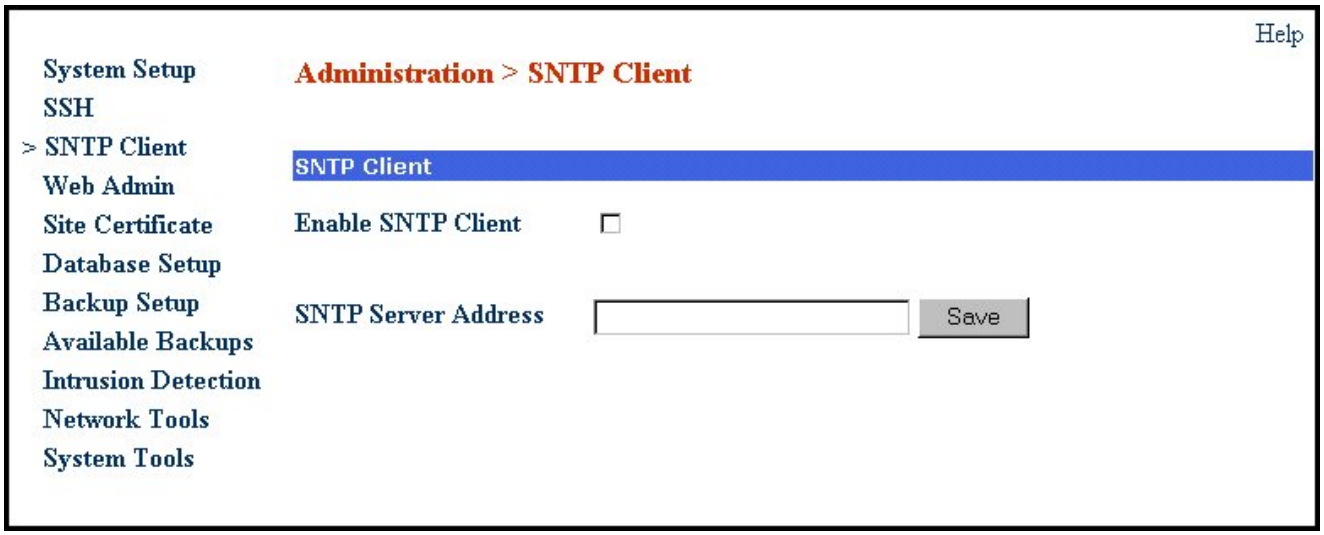
The networks that are to be allowed to access the MultiAccess using SSH must be enabled.

The default setting **Any** in **Allowed Networks** means everyone is allowed to access the SSH service. Networks are be defined in **Networks & Services > Networks** menu**.**

Caution: The default setting (**Any**) allows everyone to access the SSH service. For security reasons we recommend that you restrict the access to the SSH service. You should delete access from all other networks!

Administration > SNTP Client

SNTP (Simple Network Time Protocol) is an Internet protocol used to synchronize the clocks of computers to the same time source. Clicking the SNTP Client check box enables the MultiAccess to act as a SNTP client.



SNTP Client

Check the SNTP Client box to activate SNTP Client.

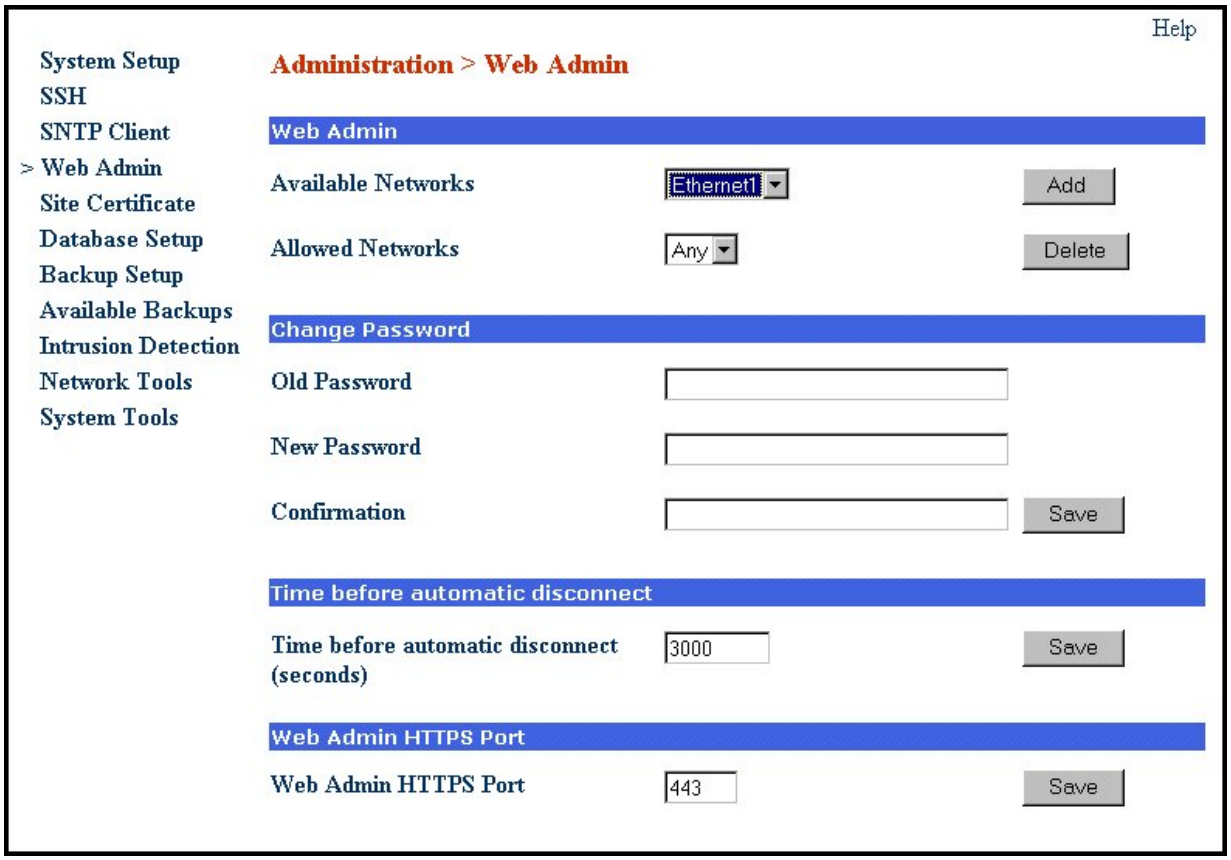
SNTP Server Address

Enter the IP address of the SNTP Server for which the firewall will contact to synchronize its clock. Then click the **Save** button.

Administration > Web Admin

From this screen you can regulate **Web Admin** access. The **Web Admin** interface uses the Secure HTTP protocol (S-HTTP, aka HTTPS) for secure transactions. Secure HTTP provides communication between your browser and the MultiAccess.

S-HTTP supports end-to-end secure transactions, in contrast with the original HTTP authorization mechanisms, which require the client to attempt access and be denied before the security mechanism is employed. With S-HTTP, no sensitive data need ever be sent over the network in the clear. S-HTTP provides full flexibility of cryptographic algorithms, modes, and parameters.



Web Admin

Available Networks

Select the networks that will allow access to Web Admin. The list includes those networks you entered under **Networks & Services > Networks**. You can add and delete existing selections. The MultiAccess will display an ERROR message if you try to delete access to a network that would cause you to lock yourself out or otherwise not make sense.

Allowed Networks

As with SSH, **Any** has been entered here for ease of installation. **ANY** allows Web Admin to be accessed from everywhere once a valid password is provided.

Caution: As soon as you can limit the location from which the MultiAccess is to be administered (e.g., your IP address in the internal network), replace the entry **ANY** in the Allowed Networks with a smaller network. If you want only one administrative PC to have access to the MultiAccess, you can do this by defining a network with a address of a single computer from the **Networks and Services > Networks** screen.

Change Password

You should change the password immediately after initial installation and configuration, and also change it regularly thereafter. Only alphanumeric characters are allowed. To change the password, enter the existing password in the Old Password field, enter the new password into the New Password field, and confirm your new password by re-entering it into the Confirmation entry field.

Caution: Use secure passwords! For example, your name spelled backwards is not secure enough; something like **xfT354** is better.

Time Before Automatic Disconnect

An automatic inactivity disconnection interval is implemented for security purposes. In the Time Before Automatic Disconnect entry field**,** enter the desired time span (in seconds) after which you will be automatically disconnected from Web Admin if no operations take place.

After the initial installation, the default setting is 3000 seconds. The smallest possible setting is 300 seconds. If you close the browser in the middle of an open Web Admin session without leaving Web Admin via Logout, the last session stays active until the end of the time-out.

If you do not logout, the next attempt to login, during the unexpired duration, will give you a pop-up stating “someone else is logged in – Do you want to kick them out?

WebAdmin HTTPS Port

HTTPS Port

This field is for setting the HTTPS port for Web administration. After setting the HTTPS port, the connection is terminated. The browser settings have to be changed for the new port number before starting the next session. By default, port 443 is configured for HTTPS sessions. The value of the port number should lie between 1 and 65535. Well known ports and ports already used by the MultiAccess are not allowed.

Administration > Site Certificate

Public keys are used as the encryption algorithm for security systems. For the validity of public keys, certificates are issued by a Certificate Authority. The Certificate Authority certifies that the person or the entity is authenticated and that the present public key belongs to that same person or entity. As the certificate contains values such as the name of the owner, the validity period, the issuing authority, and a stamp with a signature of the authority, it is seen as a digital pass. On this screen, you enter server certificate information, which the MultiAccess needs to authenticate itself to your browser. After saving the settings, the browser's security information settings have to be cleared.

Certificate Information

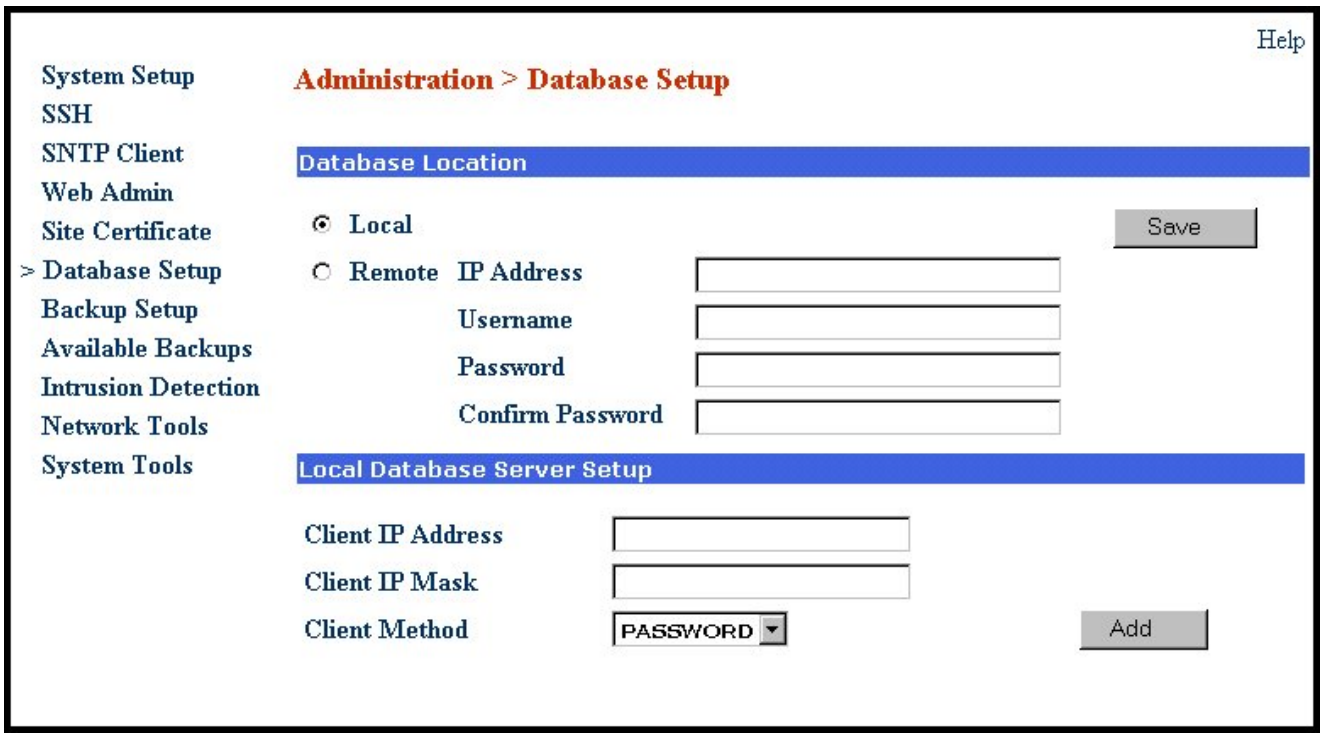
Country Code - Use the default (United States) or change to the country of operation.
State or Region - Type the state, province, region of operation.
City - Type the city name.
Company - Type the company name.
Organization Unit - Type the organizational unit (e.g., Sales & Marketing).
Contact Email - Type the email address of the contact for MultiAccess certificate data (e.g., the MultiAccess administrator) over the default (myname@mydomain.com).
Firewall Host Address - Enter the MultiAccess's host address. Use the same address that you will use to access the Web Admin interface. It can be one of the MultiAccess IP addresses.
Example: If you access Web Admin with https://192.168.10.1, the MultiAccess Host Address must also be **192.168.10.1**. If you access Web Admin with a DNS host name (e.g., https://MultiAccess Communications Server.mydomain.com), then use this name instead.

When you have entered the values, click **Save**. The browser will reconnect to the MultiAccess. At the security Alert screen, click **View Certificate.** Then click **Install Certificate** if you have not previously installed it:

1. When the first screen displays, click the **Install Certificate** button.
2. On the Welcome to Certificate Import Wizard screen, click the **Next** button.
3. On the Certificate Manager Import Wizard screen, click **Next**. You can elect to have the certificate automatically placed into a directory or you can Browse and choose your own directory. If you elect to place all certificates into a selected location, follow the on-screen prompts for Select Certificate Store, Physical Stores, and Root Stores.
4. When the certificate has been added to the Root Store, the Completing the Certificate Manager Import Wizard displays. Click **Finish**.

Administration > Database Setup

Database Setup defines where the call history database is located and maintained. If the database is to be located on this machine and other MultiAccess units are joining the data base as clients, you will need to provide client access by entering the Client IP Address, Mask, and the access method. If the database is located on a remote machine, you will need to provide the IP address of the remote machine, and appropriate user name and password.



Database Location

Selects where the database is located, Local or Remote. If the database is located on this machine, select Local. If the database is located on a remote machine, select Remote and provide the IP Address of the remote machine, and the Username and Password.

Local Database Server Setup

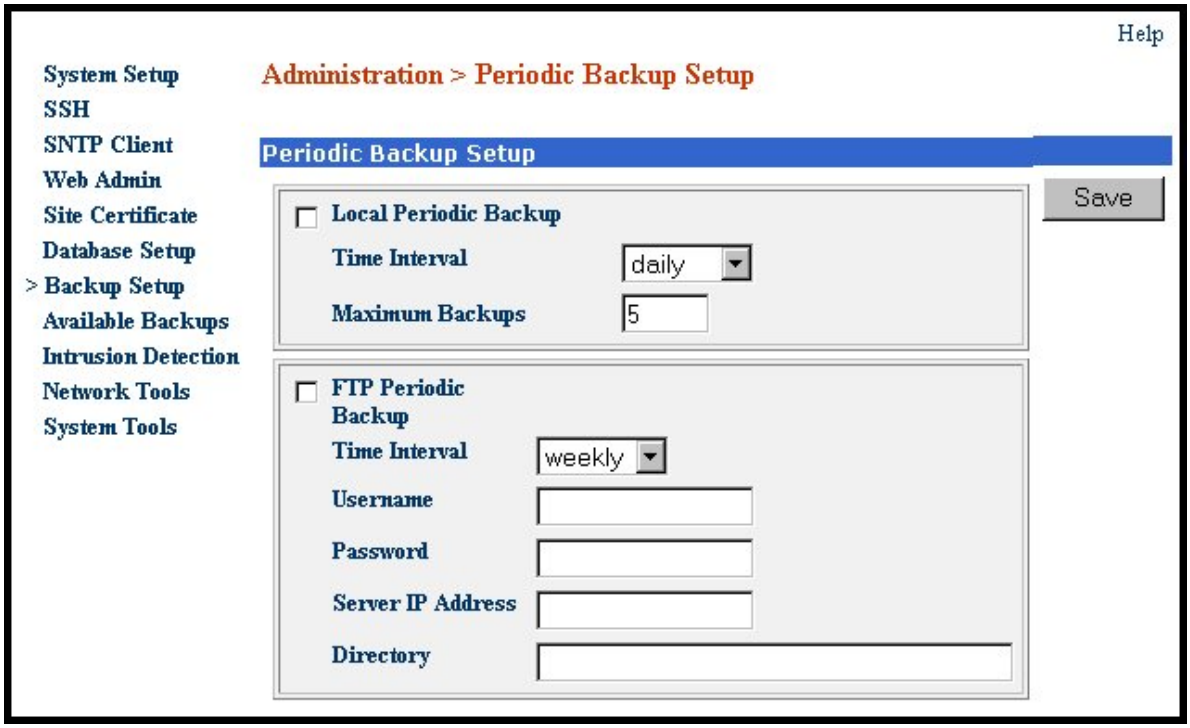
The Local Database Server Setup allows you to setup client access for the remote servers that will be sending call history records to this data base. The IP address along with the mask allows you to determine which clients are provided access to the database. The Client Method can be password, trust, reject, or md5.

Administration > Backup Setup

The Backup Setup allows you to enable and control specific aspects of the periodic back-up process. This process allows you to save your settings as .tar file either on your local system or up loaded to an FTP server. The Backup process consists of copying hundreds of configuration files into one .tar file. The .tar is then zipped and named per "config-year month day hour minute.tar.gz".

When a periodic backup is enabled, the backup occurs approximately 16 minutes after midnight, per the selected interval.

The Backup file is useful in crash recovery/system restoral situation and handy for setting up fail-safe spares. The specific configuration files that get backed up are listed in the file called "backup" located in the /opt/multi-access/data/directory. Backups will fail if this file is renamed or missing from this directory.



Local Periodic Backup

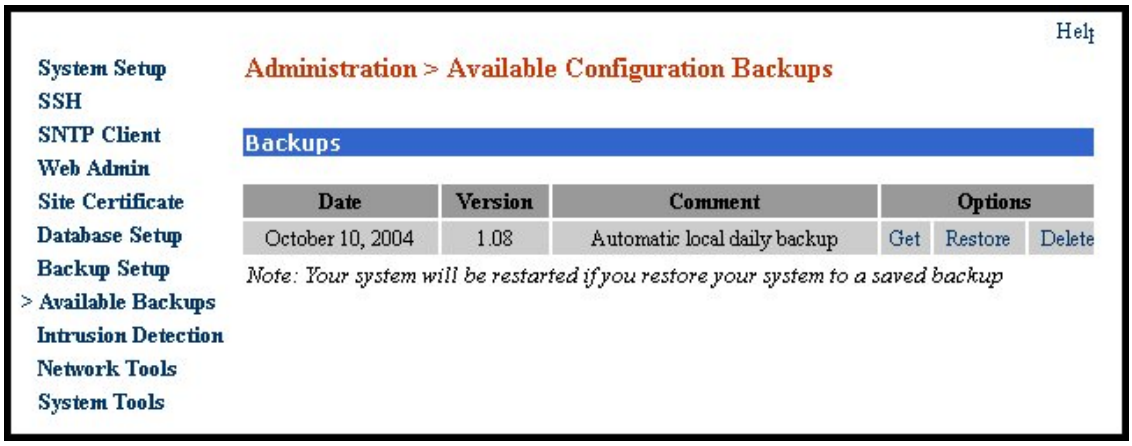
If Local Periodic Backup is chosen, the Time Interval can be selected as a daily, weekly, or monthly backup. The number set in the Maximum Backups is the number of backups that are saved on your system.

FTP Periodic Backup

If FTP Periodic Backup is chosen, the backup is uploaded to the FTP server designated in the Server IP Address field and a specific Directory can be designated in the Directory field. The Time Interval can be selected as daily, weekly, or monthly. A weekly FTP backup is the default. The backup can be security protected by using a Username and Password protection. The username and password are FTP Client credentials used to log into the FTP server. The credentials must have write access on the FTP server.

Administration > Available Backups

Available Backups allow you restore a previous saved configuration. The number set in the Maximum Backups field in the Backup Setup determines the number of backups listed here.



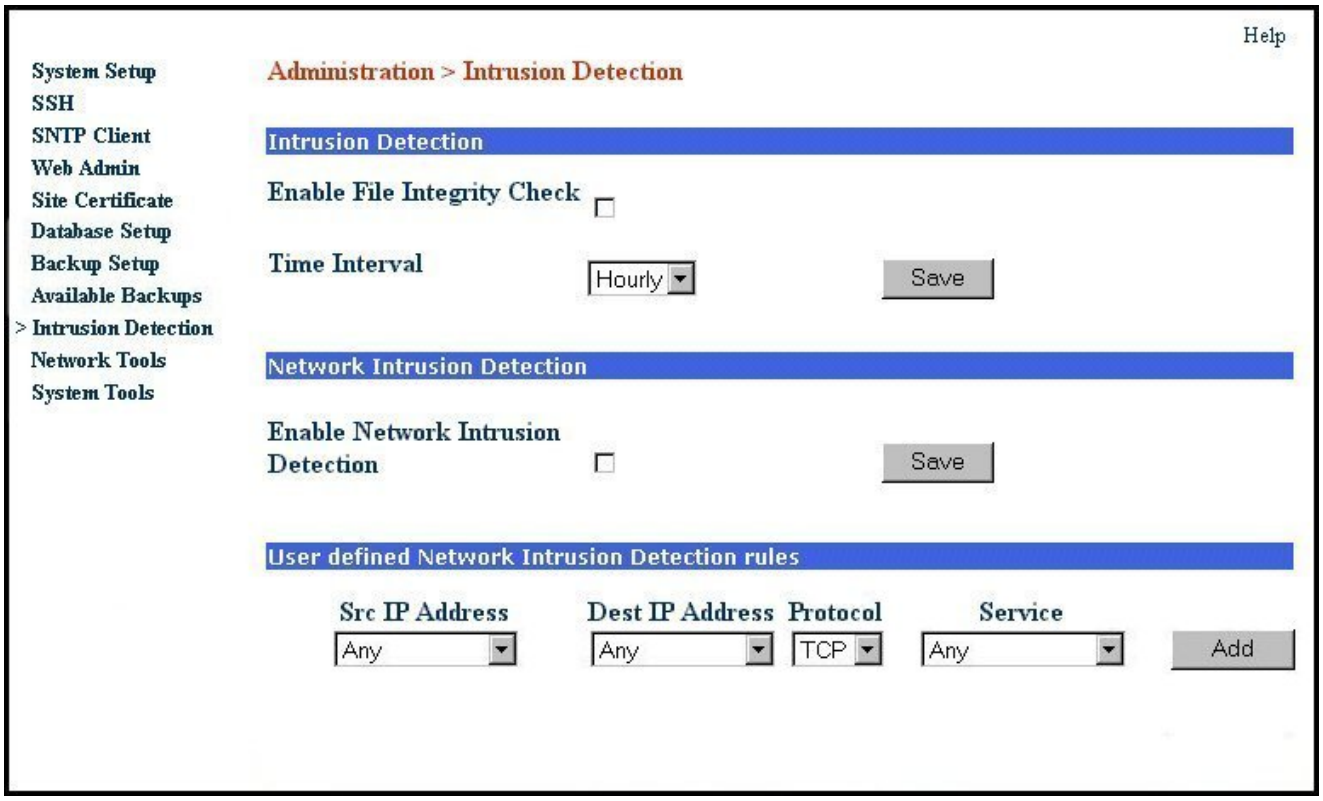
Backups

You can Get, Restore, and Delete backups. To Restore a backup, simply click on the Options Restore. Your system will be restored from the file and rebooted. To Delete a backup, click on the Options Delete and the file is removed from your system.

For situations when you want to use the backup that is on the FTP server, manually copy/get the file and place it into the /var/log/backup directory. Then it will be listed as a available configuration backup.

Administration > Intrusion Detection

The Intrusion Detection mechanism is used to notify the administrator if there has been any tampering with the files on the server.



Intrusion Detection

Enable File Integrity Check

Check the box to enable File Integrity Checking. Select the amount of time you would like the system to conduct this check. Options are every 5 Minutes, Hourly, or Daily. Then click the **Save** button.

Network Intrusion Detection

Enable Network Intrusion Detection

This allows the user to detect attacks on the network. In the event that a port scan is carried out by hackers who are looking for the weak spots in a secure network. This feature informs the administrator by email as soon as the attack has been logged. The administrator can decide what actions are to be taken. By default, DOS attack, minimum fragmentation checks, port scans, DNS attacks, bad packets, overflows, chat accesses, Web attacks will be detected; and then the administrator is informed. Apart from the above, the user can configure user defined rules for intrusion detection.

Check the box to enable Network Intrusion Detection. Then click the **Save** button.

User Defined Network Intrusion Detection Rules

SRC IP Address

This selection allows you to choose the network from which the information packet must be sent for the rule to match. Network groups can also be selected. The ANY option matches all IP addresses, regardless of the whether they are officially assigned addresses or private addresses. These Networks or groups must be predefined in the Networks menu.

Destination IP Address

This selection allows you to choose the network to which the information packet must be sent for the rule to match. Network groups can also be selected. These network clients or groups must have been previously defined in the Networks menu.

Protocol

This selection allows you to choose the type of protocol, i.e., TPC or UDP.

Service

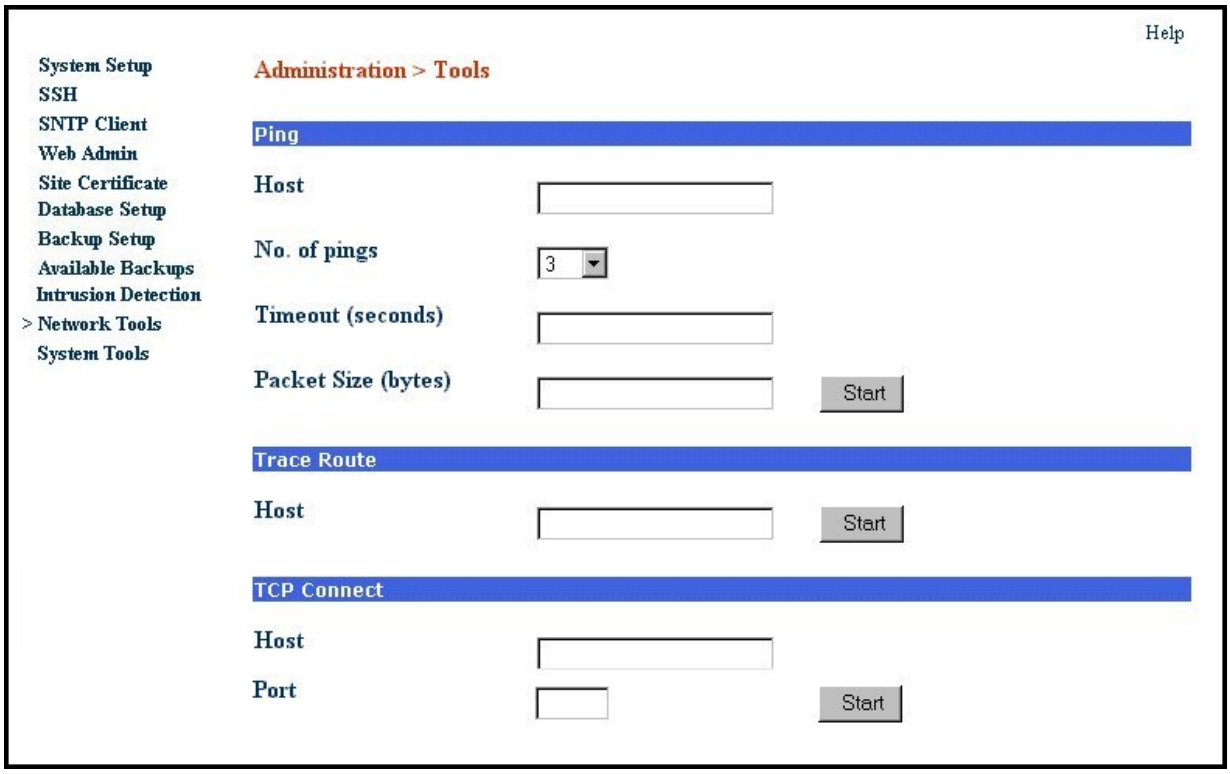
This selection allows you to choose the corresponding service. The service must have been previously defined in the Services menu. Select intrusion detection rules from the following dropdown list boxes:

Add

After the rules are defined/selected, click the **Add** button. The commands can be deleted by clicking **Delete** under the Command option.

Administration > Network Tools

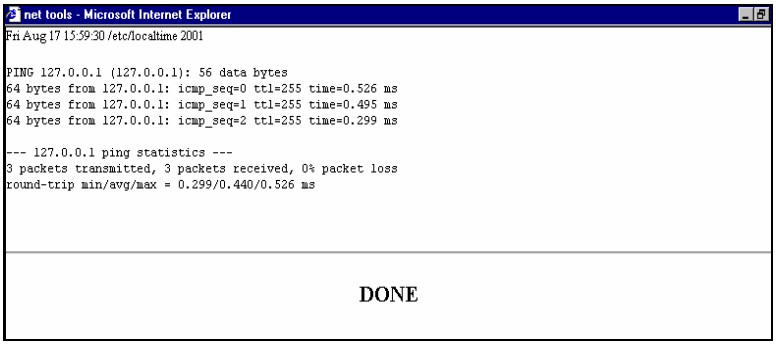
There are three tools that can help you test the network connections and functionality. Ping and Trace Route test the network connections on the IP level. TCP Connect tests TCP services for availability.



PING

Ping is an acronym for Packet Internet Groper. The PING utility is used as a diagnostic tool to determine if a TCP/IP communication path exists to a remote host. The utility sends a packet to the specified address and then waits for a reply.

Host - Specify the IP address or name of the other computer for which connectivity is to be checked.
Number of PINGS - Select the number of pings. You can choose 3 (the default), 10 or 100 pings.
Timeout - Specify the duration to wait before declaring “timeout, “no response”.
Packet Size (bytes) - Specify the number of data bytes to be sent.
Start - After clicking the Start button, a new browser window opens with the PING statistics accumulating.


net tools - Microsoft Internet Explorer
Fri Aug 17 15:59:30 /etc/localtime 2001
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=0.526 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=0.495 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=255 time=0.299 ms
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.299/0.440/0.526 ms
DONE

Trace Route

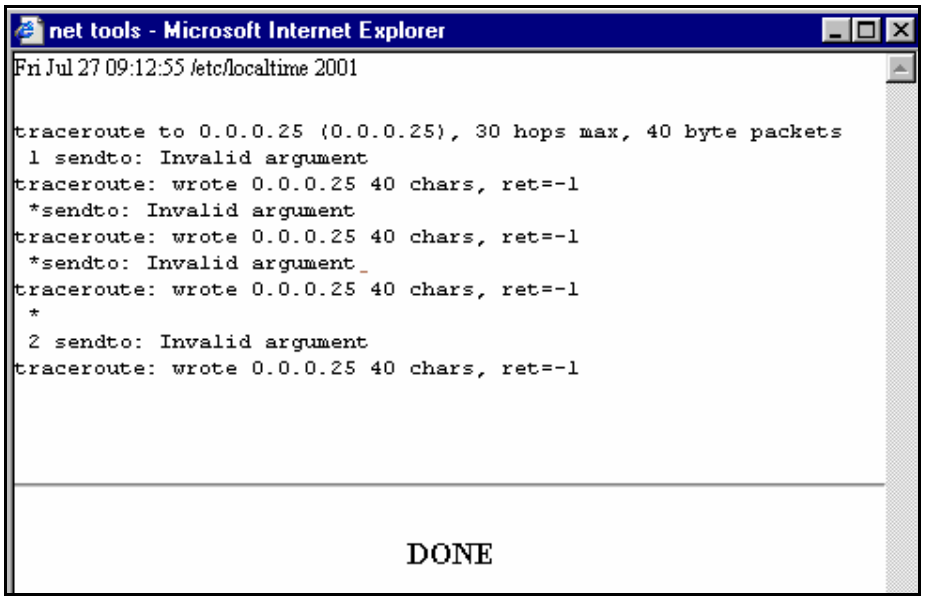
Trace Route is a tool for finding errors in the network routing. It lists each router/hop/network on the way to remote host. If the path for the data packets is temporarily unavailable, the interruption is indicated by asterisks (*****). After a number of tries, the attempt is aborted. The interrupted connection can have many causes, including the packet filter on the MultiAccess not allowing the operation of Trace Route.

Host

Specify the **IP address** (host name) of the other computer to test this tool.

Start

Click the corresponding **Start** button to start the test.


net tools - Microsoft Internet Explorer
Fri Jul 27 09:12:55 /etc/localtime 2001
traceroute to 0.0.0.25 (0.0.0.25), 30 hops max, 40 byte packets
1 sendto: Invalid argument
traceroute: wrote 0.0.0.25 40 chars, ret=-1
*sendto: Invalid argument
traceroute: wrote 0.0.0.25 40 chars, ret=-1
*sendto: Invalid argument
traceroute: wrote 0.0.0.25 40 chars, ret=-1
*
2 sendto: Invalid argument
traceroute: wrote 0.0.0.25 40 chars, ret=-1
DONE

A Sample Trace Route Log

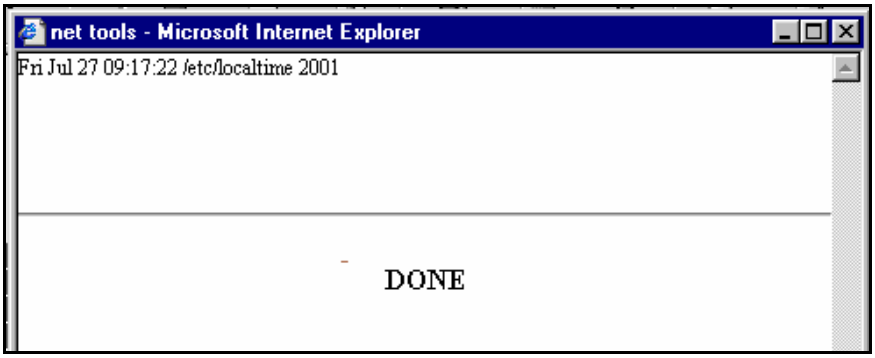
TCP Connect

This system tool tests specific TCP ports for availability between the source MultiAccess and destination addresses.

Host – Enter the IP address or host name of the destination.
Port – Enter the port number in the Port window. For example, port number 23 for telnet service.
Start – Start the test connection by clicking the **Start** button.

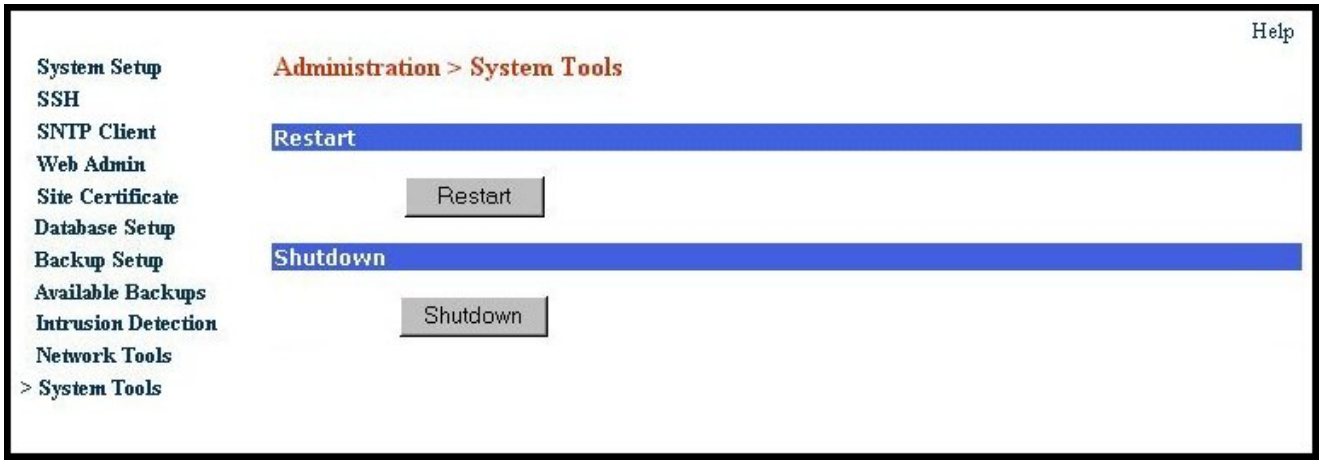
The results are:

- Connected to host
- Connection refused by host
- Not route to host



Administration > System Tools

System tool includes Restart, and Shutdown. Restart allows the MultiAccess to be shut down and restarted. Shut down ensures that all services are shut down correctly.



Restart

By clicking the Restart button, the MultiAccess is shut down and rebooted. The message **Are you sure you want to restart the system?** is displayed. By clicking the **OK** button you confirm that you want to restart the MultiAccess. The login screen displays while the restart process takes place. The unit is first brought to run level 0, which takes approximately 30 seconds to reach. At this point the system BIOS is restarted and the unit begins to boot up. You will be able to log back in when run level 3 has been reach, which usually takes about 2 minutes. However the boot up process is subject to a number of variables that could dramtically increase the time needed to reach run level 3.

Shutdown

This tool should be used when AC power is to be removed from the unit (moving the unit or adding MA30EXP expansion modules). Clicking the Shutdown button starts the shutdown process. The message **Are you sure you want to shut down the system?** is displayed. By clicking the **OK** button you confirm that you want to shutdown the MultiAccess. The login screen displays while the shutdown process takes place. When a proper shutdown is initiated, immediately 1 beep is heard and then the unit starts to shutdown (killing services, unloading driver, etc) and then approximately 30 seconds later “run level zero” is reached and two consecutive beeps are heard, after which it is now safe to power off the unit.

Caution: Avoid improper shutdowns. You should switch off the MultiAccess’s power only after you have completed the shut down process. Improper shutdowns will increase the start up time on the subsequent boot up. They can in some cases cause or lead to hard drive failures.

Note: Upon initial power up, within 5 seconds one beep is heard at a successful POST of the BIOS, approximately 90 to 120 seconds later five consecutive beeps will be heard when the system has reached run level 3. During the boot up time all 12 line interface LEDs will simultaneously flash on/off (repeatedly), until run level 3 is reached. Line interface and modem drivers take up to an additional 60 seconds to load after run level 3 has been reached. When the line interface and modem drivers finish loading, only the activated line interfaces will have appropriate LEDs illuminated.

The time needed to fully boot up is a variable depending on the number of modem modules installed, hard drive variables (journal events and file system checks) and other Linux system variables.

In some rare occasions, timing variables to the shutdown process may result in not all PIDs being removed.

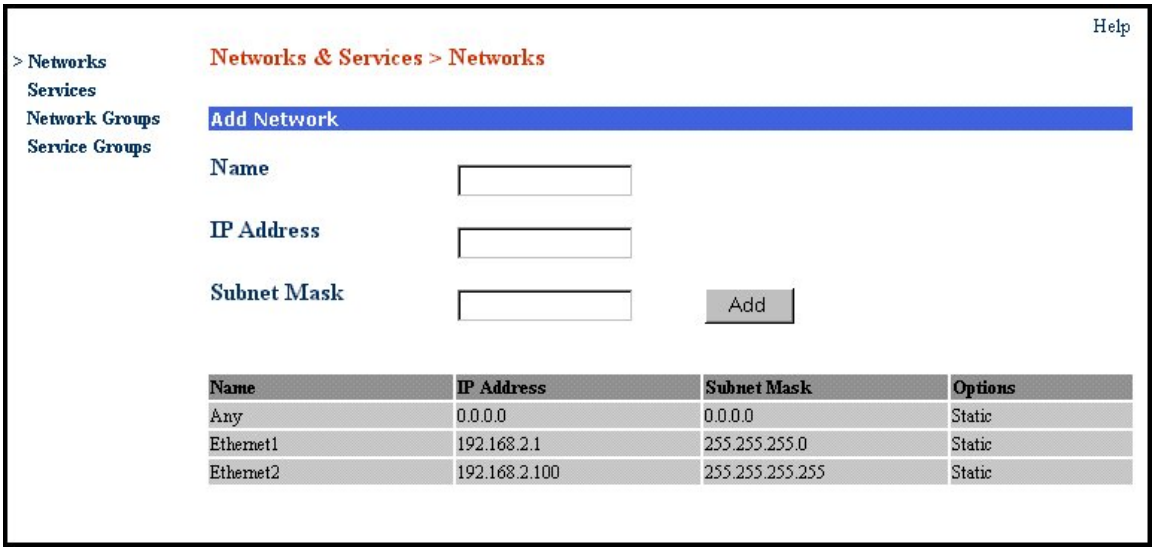
Networks & Services

Networks & Services > Networks

A network consists of a unique name, an identifying network number, and a Subnet Mask. Once you add a network, the information displays at the bottom of the screen. This network table contains the default networks which cannot be deleted or edited.

Important Notes:

- IP address (network number) will change if changes are made to the IP addresses in Network Setup of Ethernet 1 and Ethernet 2.
- To define a single host, enter its IP address and use a netmask of 255.255.255.255. Technically, single hosts are treated in the same way as networks.
- A network or host you added can be deleted only if it is not used for any route or by any other module.
- If a network process/function is using a network, that network cannot be edited. Similarly, if a host address is edited and changed, and if that host was used by SNAT or DNAT, the change will not be performed.



Add Network

Name

Enter a straightforward name into the Name entry field. Networks can be used to set packet filter rules, static routes, etc.. Accepted characters: alphabetic, numerical 0 to 9, the minus sign, and underscore. Forward slash and backward slash are not accepted as a valid character. Maximum characters are 39.

IP Address

Enter the network number (e.g., 192.168.3.0).

Subnet Mask

Enter the Net Mask. Subnet mask 255.255.255.0. Defines a private Class-C net.

Confirm your entries by clicking the **Add** button. After a successful definition, the new network is entered into the network table. This network will now be referenced in other menus under this name. You can edit and delete networks by clicking **Edit** or **Delete** in the **Options** column for the network you want to change. The name of the network can not be changed, but the IP Address and Subnet Mask can be edited. You can delete a newly created network by clicking on **Delete** in the Options column for a desired network.

Added networks are displayed in the following functions:

1. Web Admin
2. SSH
3. Packet Filter Rules
4. Network Intrusion Detection
5. Routing
6. Masquerading
7. SNAT
8. DNAT

These names will be made available to:

1. Add allowed networks for Web Admin
2. Add packet filter rules
3. Add source, destination networks for Network Intrusion Detection
4. Add routes in routing, SNAT, masquerading, portscan detection and DNAT sections.

Networks & Services > Services

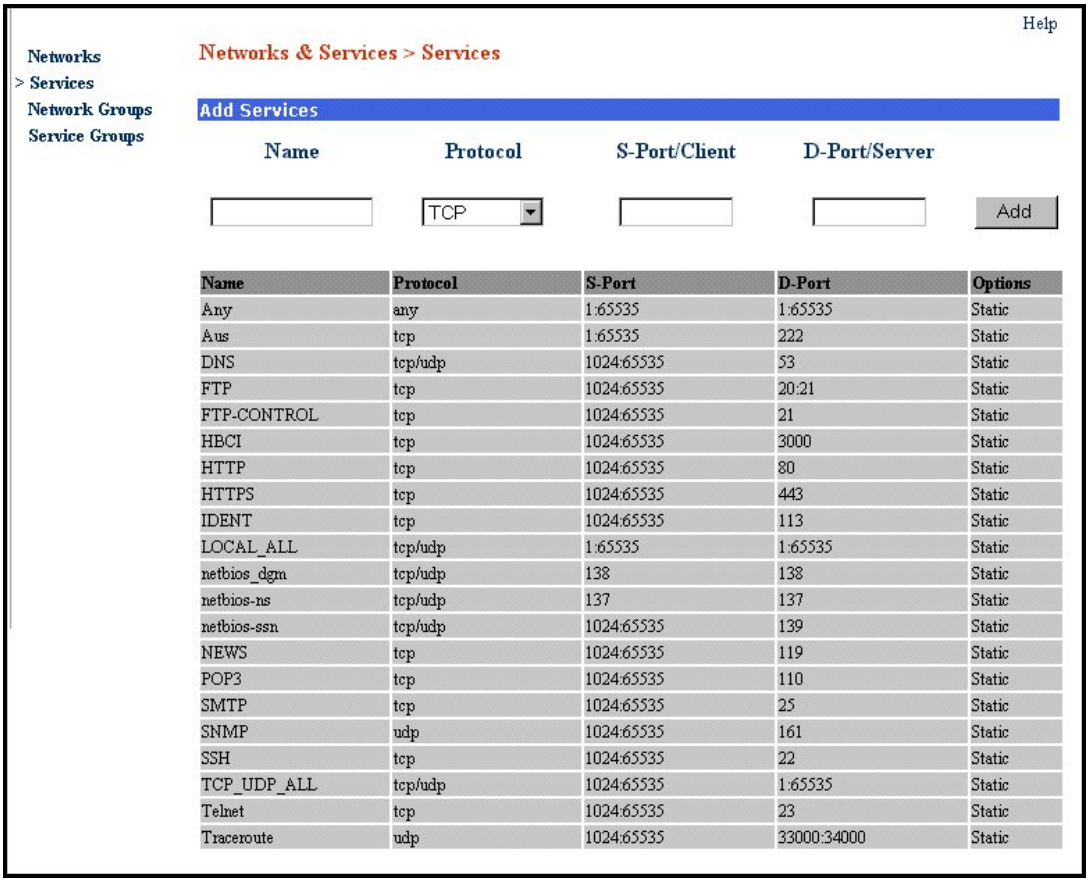
On this screen you can set the MultiAccess protocol services. Protocols make ongoing administration easier. You will define data traffic as it travels the networks (e.g., the Internet). A service protocol setting consists of a **Name**, the **Protocol**, the **S-Port/Client** (source port), and the **D-Port/Server** (destination port).

When entering the ports, you can enter a single port or a port range separated by a colon (:).
For **AH** and **ESP**, the **SPI** is a whole number between 256 and 65536, which has been mutually agreed upon by the communication partners. The Internet Assigned Numbers Authority (IANA) reserves values below 256.

Notes:

- **TCP & UDP** allow both protocols to be active at the same time. **Any** causes the MultiAccess to accept any protocol offered.
- The **ICMP** protocol is necessary to test network connections and MultiAccess functionality, as well as for diagnostic purposes. In the **Packet Filter > ICMP** menu you can enable **ICMP Forwarding** between networks, as well as MultiAccess ICMP reception (e.g., to allow **ping** support).
- The **ESP** protocol is required for Virtual Private Network (VPN).
- The **AH** protocol is required for Virtual Private Network (VPN).

There are options for editing or deleting the user added services. However, there are some standard services, which cannot be edited or deleted. If the Packet Filter rules, SNAT, or DNAT uses the service, it cannot be deleted. For editing any user-defined service, the **Edit** button has to be clicked to get the fields corresponding to the service entry. The entries can be saved using the **Save** button.



Name	Protocol	S-Port	D-Port	Options
Any	any	1:65535	1:65535	Static
Aus	tcp	1:65535	222	Static
DNS	tcp/udp	1024:65535	53	Static
FTP	tcp	1024:65535	20:21	Static
FTP-CONTROL	tcp	1024:65535	21	Static
HBCI	tcp	1024:65535	3000	Static
HTTP	tcp	1024:65535	80	Static
HTTPS	tcp	1024:65535	443	Static
IDENT	tcp	1024:65535	113	Static
LOCAL_ALL	tcp/udp	1:65535	1:65535	Static
netbios_dgm	tcp/udp	138	138	Static
netbios-ns	tcp/udp	137	137	Static
netbios-ssn	tcp/udp	1024:65535	139	Static
NEWS	tcp	1024:65535	119	Static
POP3	tcp	1024:65535	110	Static
SMTP	tcp	1024:65535	25	Static
SNMP	udp	1024:65535	161	Static
SSH	tcp	1024:65535	22	Static
TCP_UDP_ALL	tcp/udp	1024:65535	1:65535	Static
Telnet	tcp	1024:65535	23	Static
Traceroute	udp	1024:65535	33000:34000	Static

Add Services

Name
Enter a unique name in Name entry field. You will need this later (e.g., to set packet filter rules).

Protocol
Select from the following protocols: **TCP, UDP, TCP & UDP, ANY, ICMP, AH, and ESP**.

ICMP Type
Select the **ICMP type** (e.g., echo reply**,** echo request**,** time to live exceeded, etc.). It will display if the protocol type is ICMP>

ICMP Code
Select the **ICMP code** (e.g., all). It will display if the protocol type is ICMP and the ICMP Type is redirect network, network unreachable, to time to live exceeded.

S-Port/Client (Source Port)
Enter the source port for the service. The entry options are a single port (e.g. 80), a list of port numbers separated by commas (e.g. 25, 80, 110), or a port range (e.g. 1024:64000) separated by a colon (**:**). It will be displayed if the type of the protocol is TCP, UDP, TCP+UDP, or ANY.

D-Port/Server (Destination Port)
Enter the destination port for the service. It will be displayed if the type of the protocol is TCP, UDP, TCP+UDP, or ANY.

Add Button
After you have entered the service, click the **Add** button.

Edit
By clicking **Edit** in the Options column, the information is loaded into the entry menu of the **Edit Service** screen. You can then edit the entry. You can edit user-added services; however, there are some standard services that cannot be edited.

Delete
By clicking **Delete** in the Options column, the service is deleted from the Services table. You can delete user-added services; however, there are some standard services that cannot be deleted. If Packet Filter rules, SNAT, or DNAT uses a service, it cannot be deleted.

Important:

The user added services are displayed in the following functions:

1. Packet Filter Rules
2. Network Intrusion Detection
3. SNAT
4. DNAT

The user added services are available to:

1. Add packet filter rules
2. Add specific services for Network Intrusion Detection.
3. Add rules in SNAT and DNAT functions.

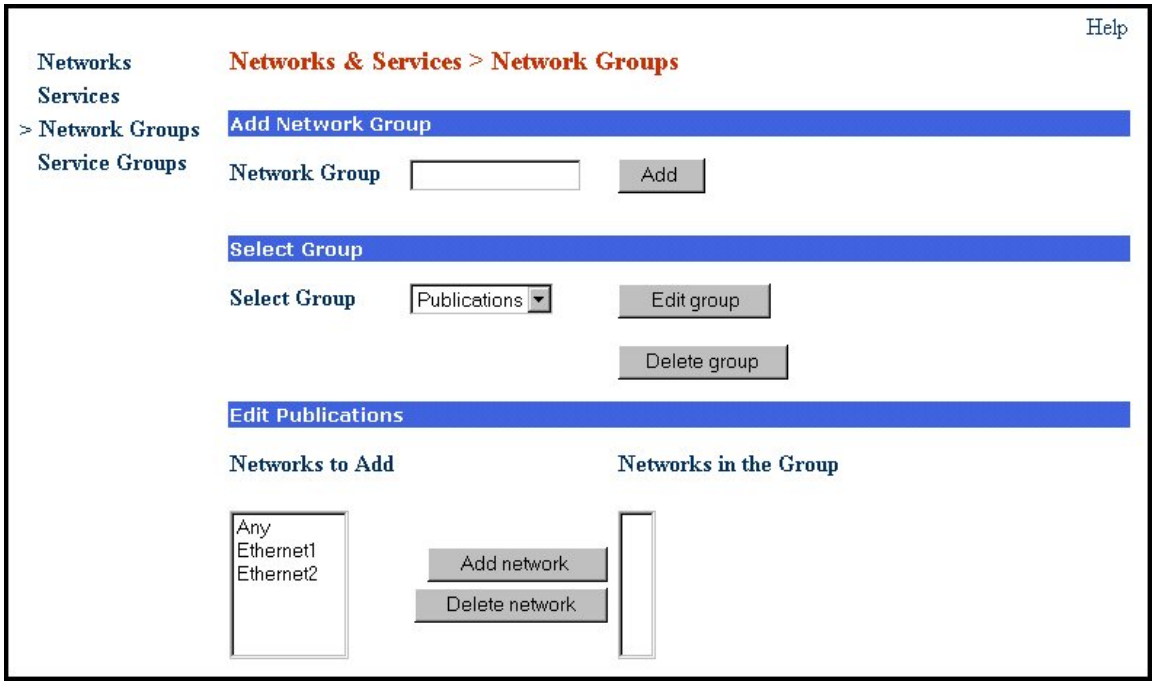
Networks & Services > Network Groups

On this screen you can group various networks into a group. The networks that were added in the **Network & Services > Networks** section can be placed into a group.

A network, which is already a part of a group, cannot be added to any other group. It is suggested that you start a group name with a **G-** or **Group-**. This will identify group network names in contrast to network names.

When editing Network Groups, note that by pressing the **Shift** key, several entries can be marked together allowing them to be added or deleted together.

Note: Every change in Network Groups is effective immediately.



Add Network Group Name

Network Group

Enter a unique name for the network group in **Add Network Group**. This name is used later if you want to perform operations such as setting packet filter rules. Confirm your entry by clicking the **Add** button.

Select and Edit the [Group Name Selected Above Displays]

Click the **Edit Group** button to add networks to a group. The group for which the networks have to be added has to be selected from the box. When the **Edit Group** button is clicked, the list of all the networks, which are not part of any group, and the list of networks which fall under that group will be displayed.

Delete the Group

The **Delete** button must be clicked to delete the group selected.

Adding Networks to a Group

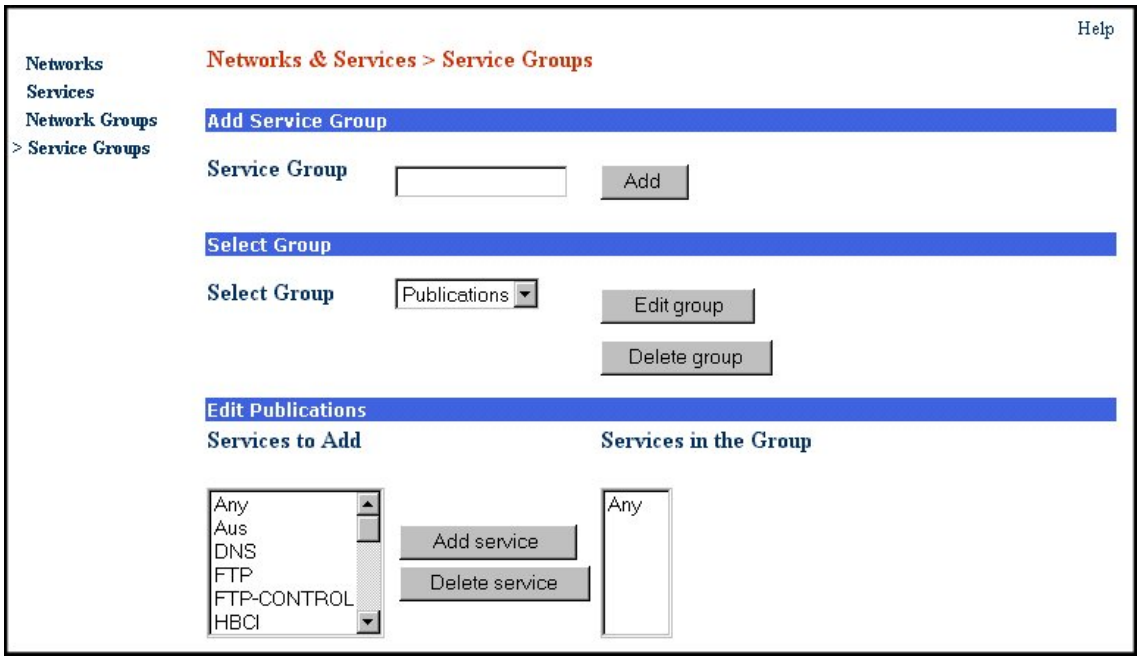
This option will be available if the **Edit Group** button is clicked. The groups can be selected from the list of networks displayed to the left of the **Add Network** button. After selecting the networks (multiple selections can be done), the **Add Network** button must be clicked to add the networks to the selected group.

Deleting Networks from a Group

This option will be available if the **Edit Group** button is clicked. The networks to be deleted can be selected from the list of networks displayed to the right of the **Delete Network** button. After selecting the networks (multiple selection can be done), the **Delete Network** button must be clicked to delete the networks from the selected group.

Networks & Services > Service Groups

On this screen you can combine multiple Services (see Services section) into groups, called Service Groups. **Service Groups** are treated like single services. A service that is already a part of a group cannot be added to any other group. A service can also be deleted from a group.
Note: Every change made to **Service Groups** is effective immediately.



Add Service Group Name

Assign a unique name for the **Service Group**. This name is required for later operations such as creating a higher-level service group or to set packet filter rules. Confirm your entries by clicking **Add**. All names will be added to **Select Group** drop down list box from which you can **Edit** or **Delete** a Service Group.

Select and Edit a Group

Click the **Edit Group** button to add services to a group or delete services from a group. The group for which the services have to be added or deleted has to be selected from the **Select Group** (name) box. After clicking the **Edit Group** button, the list of all the services and the list of the services, which fall under that group, will be displayed. You can select several services at once by holding down the **Shift** key as you select them.

Delete a Group

Click the **Delete Group** button to delete a group selected from **Select Group** list.

Adding Services to a Group

This option will be available if the **Edit Group** button is clicked. The groups can be selected from the list of services displayed to the left of the **Add Service** button. After selecting the services (multiple selections can be done), click the **Add Service** button. The services from which to choose are:

ANY	Aus	IDENT	netbios-ssn	SMTP	DNS	Telnet
FTP	HTTP	netbios-dgm	NEWS	SNMP	Local_ALL	Trace Route
FTP-CONTROL	HTTPS	netbios-ns	POP3	HBCI	SSH	TCP_UDP-ALL

Deleting Services from a Group

This option will be available if the **Edit Group** button is clicked. The services to be deleted can be selected from the list of services displayed to the right of the Delete button. After selecting the services (multiple selections can be done), click the **Delete Service** button.

Network Setup

The Network Setup menus consist of Interface, Routes, Masquerading, SNAT, and DNAT screens. The Interface screen is used to set up two Ethernet interfaces with funtional IP parameters for your network or networks. Routes screen is used to define additional (network specific) IP routes. The Masquerading screen is used to hide private addresses behind public addresses. DNAT and SNAT screens are also used to hide private addresses, but with more control of a public access perspective (directional control).

About the Interface Screen

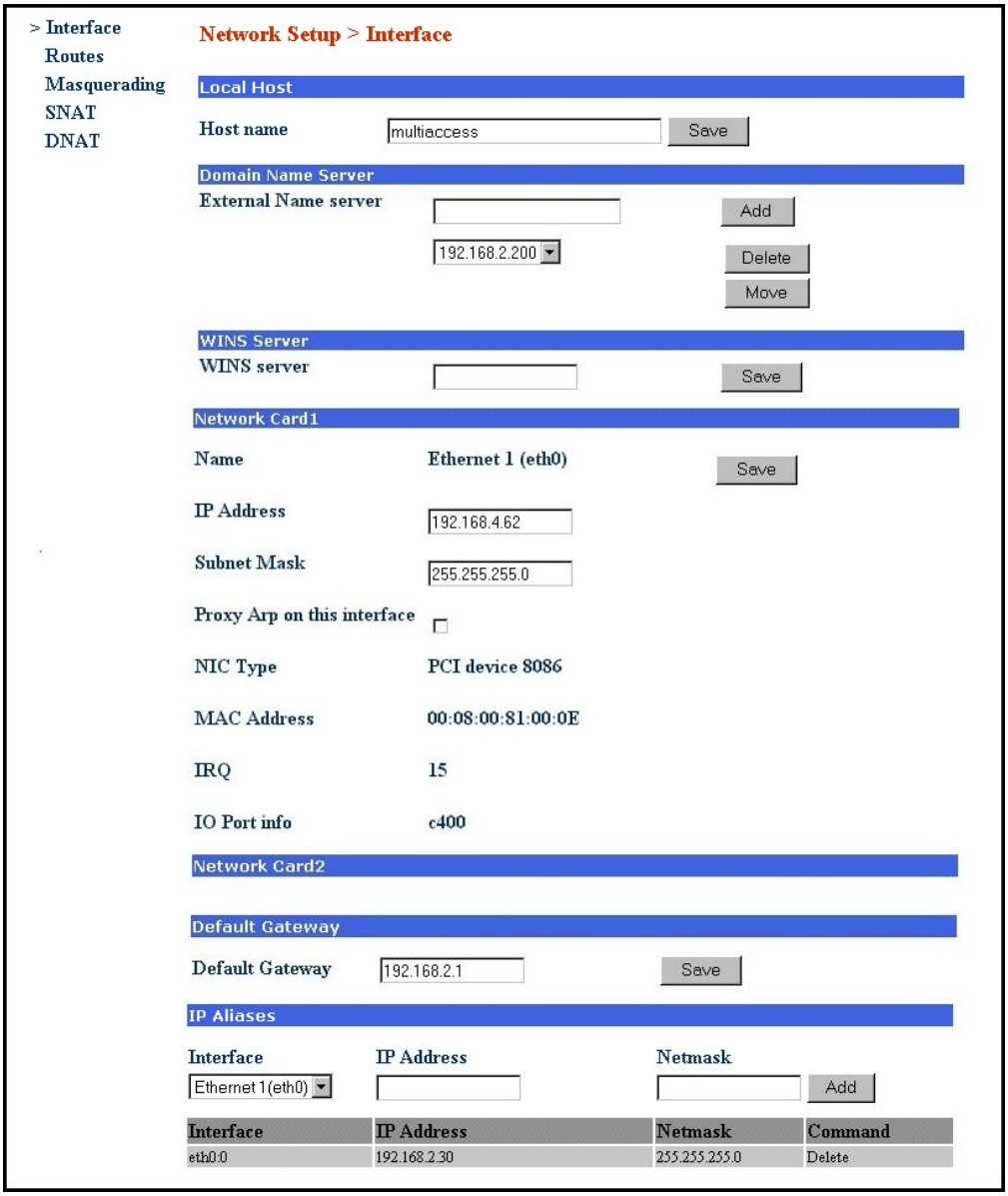
These settings are for setting the default gateway, host name, external name servers for the system, configuration of IP address, mask for the installed network cards, enabling/disabling Proxy ARP on each of the interfaces, configuring aliases for each of the interfaces.

Configure the first Ethernet interface (Network Card 1) with the basic/primary network parameters. For example, change the IP address and subnet mask of eth0 to an available, static address that matches the network this MultiAccess is going to be used on, then click on the Save button. Confirm the pop up menu regarding the address change and wait approximately 1 minute for the parameter change to take affect. Then enter the new IP address in the Address bar of your browser and proceed to log back into the unit.

Configure the remaining basic parameters; Defining the default gateway, adding at least one DNS server (this is used by the operating system to resolve names), and define a host name for the MultiAccess.

It is not necessary to configure and connect the second Ethernet interface. The intended use of the second network interface is for more advanced applications. Use of the second interface lends flexibility to separate applications, useful with private and public network implementations, provides an alternative means of network access and can aid in troubleshooting. It is acceptable to have both interfaces on the same network, as long as they have unique host addresses, or they can be on separate networks.

Network Setup > Interface



When you view this screen on your PC, you will see an additional section for entering Network Card 2 information. Since the input fields are the same as those for Network Card 1, they are not included in this graphic.

Local Host

Host Name

Enter a name for the MultiAccess into the Host Name field. An example is **MultiAccess.mydomain.com**. Click the **Save** button after entering the Host Name.

Domain Name Server

Configure the remaining basic parameters; Defining the default gateway, adding at least one DNS server (this is used by the operating system to resolve names), and define a host name for the MultiAccess.

Dial in clients use the DNS server defined in the Radius Client screen.

External Name Server

Enter the IP address of the name server in this field. Click the **Add** button. If more than one name server is to be configured, they are consulted in the order they are configured. Option to delete name servers and change the priority of name servers is also provided.

WINS Server

The WINS Server option is for the operating system, not the dial-in client.

WINS Server

Enter the IP address of the name server in this field. Click the **Save** button. If more than one name server is to be configured, they are consulted in the order they are configured. Option to delete name servers and change the priority of name servers is also provided.

Network Cards

This entry provides the static IP address for the corresponding Network Card.

IP Address and Subnet Mask

Enter the IP address and the corresponding Subnet Mask into the appropriate entry fields. For example:

Network Card 1 (eth0)	*Network Card 2 (eth1)*
Name (Description): LAN 1 IP Address: 192.168.2.1 Subnet Mask: 255.255.255.0	Name (Description): LAN 2 IP Address: 192.168.100.1 Subnet Mask: 255.255.255.0

Caution: When entering a new IP address, it is possible to temporarily "lock yourself out". If you do, you will need local console access to re-establish proper network communication.

Proxy ARP on This Interface

If you check the **Proxy ARP on This Interface** checkbox, the MultiAccess recognizes ARP request for hosts on the other side of a dial-in router. The MultiAccess answers for those addresses with an ARP reply matching the remote IP address with the MultiAccess's Ethernet address. This applies typically in situations where the routing is LAN to LAN instead of LAN to client.

NIC Type, MAC Address, IRQ, and IO Port Info

This information defaults into the corresponding fields.

Save

Confirm your settings by clicking the **Save** button.

Default Gateway

The Default Gateway has to be entered in the text field in a dotted decimal format and can be saved by clicking the Save button. The Default Gateway needs to be configured when dialed in computers, i.e., IP enabled devices, or the MultiAccess needs to communicate with other computers that are not on the same IP network (subnet). If the IP devices are all on the same subnet, they do not need to know a default gateway.

IP Aliases

From this part of the Interface screen you can add Aliase IP addresses to the network interface of the MultiAccess. With IP aliases, you can assign several additional IP addresses to a network interface. The MultiAccess will treat the additional addresses as equals to the primary network interface address. IP aliases are required to administer several logical networks on one network interface. They can also be necessary in connection with the SNAT function to assign additional addresses to the firewall.

Note: The same IP address cannot be configured many times for an interface. Similarly, the same IP address cannot be entered as an alias for two different interfaces.

Interface
From the drop down list box, select the network name to which you want to assign an alias.

IP Address
Enter the network IP address for the network named.

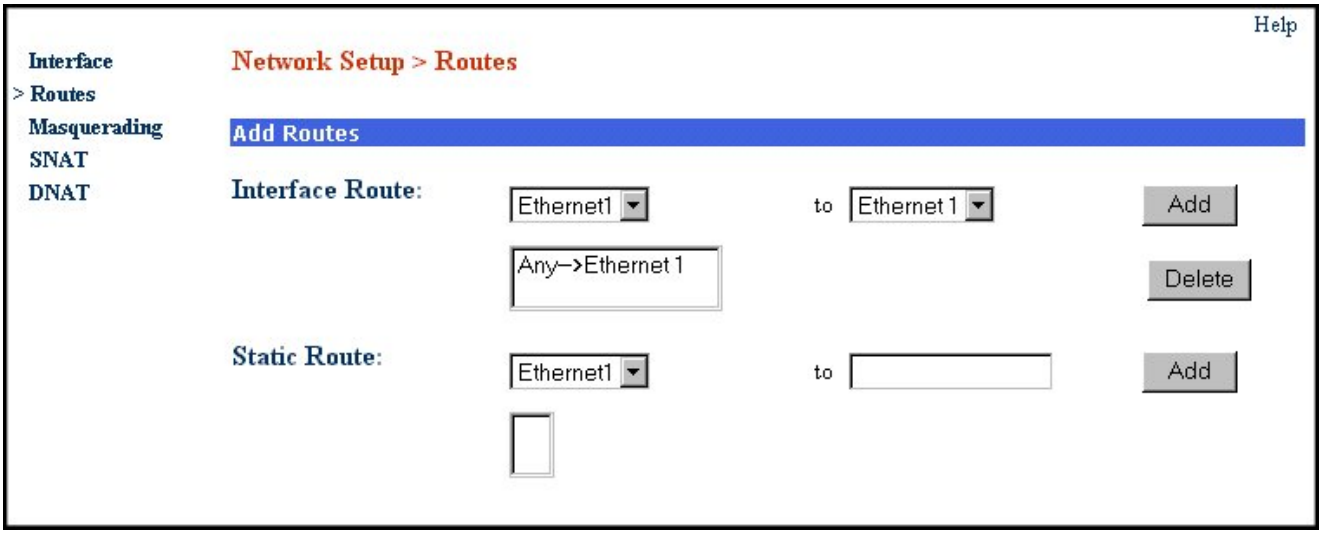
Netmask
Enter the Netmask to be used for this network.

Add
Click the **Add** button.

The IP alias is displayed in the table at the bottom of the section.

Network Setup > Routes

The Routes menu allows you to define additional IP routes. When you add a route, you are modifying the internal routing table of the MultiAccess. There are two types of routes used by the MultiAccess; Interface routes and Static routes. Depending on the situation, you may need to create just an Interface route or just a Static route, or possibly both.



Add Routes - Interface Route

Interface Route

An interface route assigns a network to an Ethernet interface. Select an already defined network and a network card. The entries are confirmed by clicking the **Add** button. Also, existing entries can be deleted by highlighting the entry and clicking the **Delete** button.

Add Routes - Static Route

A static route defines which router, external to the MultiAccess, is to be used to reach a particular destination. Select an already defined network from the drop-down list. Enter the external IP address, which will act as a gateway to this network. Confirm your entry by clicking the **Add** button. Existing entries can be deleted by highlighting the entry and clicking the **Delete** button.

Note: The specified gateway should be reachable first. This means the gateway should be on either the network of eth0 or eth1.

Delete a Route

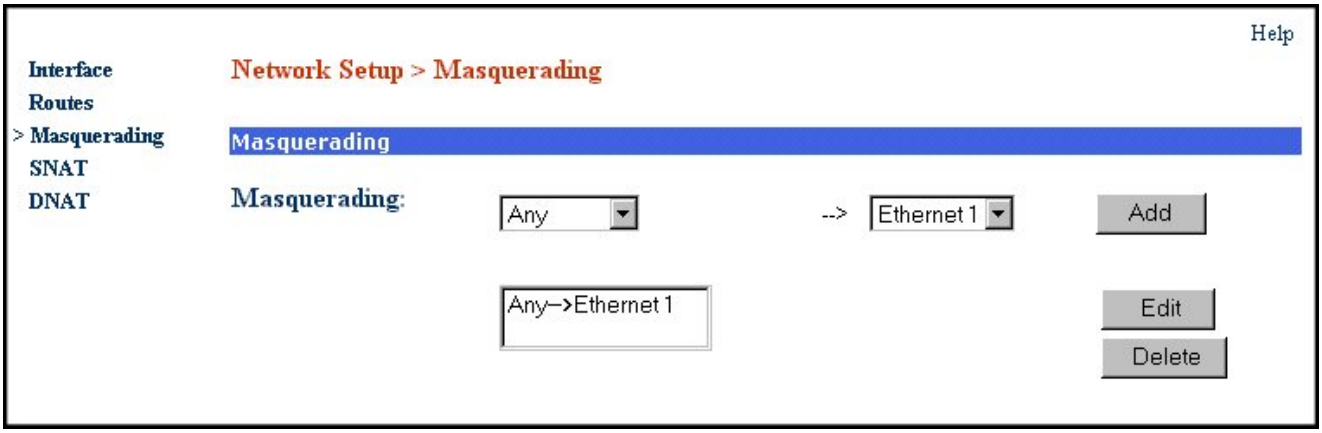
Select a Route from the table and click the **Delete** button. When deleting a Route, the interface adapts accordingly.

Note: You can view the Routing Table in **Statistics & Logs > Networks > Routing Table**.

Network Setup > Masquerading

Masquerading is a process which allows a whole network to hide behind one address. The MultiAccess can use this to your advantage by allowing dial-up users access to your private and public networks yet hiding your internal IP addresses and network information from the public network. Masquerading is also helpful when there is a limited number of available IP addresses. Masquerading translates data packets generated by the hidden network to the indicated MultiAccess network interface. All services are automatically included in the translation. The translation takes place only if the packet is sent via the indicated network interface. The addess of the MultiAccess network interface is used as the new source of the data packets.

The Network Setup > Masquerading screen allows you to select the network or group of networks to be masked to a selected network card.



Masquerading

Masquerading

Select one of the networks already defined in the Networks menu. Select a network from the box on the left and add → it to one of the Ethernet cards. Click Add.

Add

Click the **Add** button. The Masqueraded network route displays below.

Edit or Delete

Select Masqueraded network route from the lower box and click the **Edit** or **Delete** button. When deleting a Masqueraded network route, the interface adapts accordingly.

Small Office Example

Solution: Create a private network just for the dial-in users and then masquerade it to the MultiAccess interface that is on your LAN.

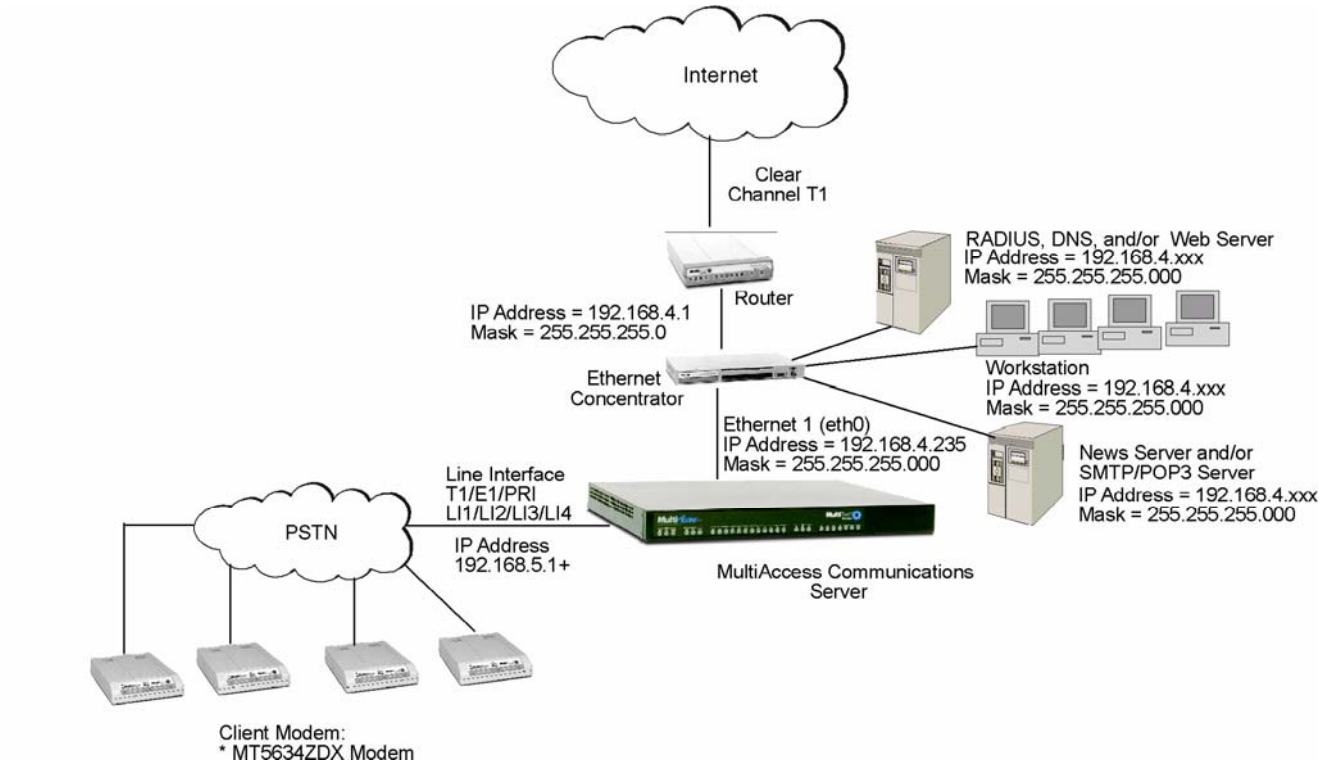
This example is based on the premise the MultiAccess is a 24-port server, full or near full capacity is expected to be reached on a regular basis and most dial-in users only require a dynamic IP address. This means the IP address pool for the dial-up connections should be a contiguous group of 24. The users that receive IP addresses from this masqueraded pool will appear on the network with their source address being the same as that of the MultiAccess.

For example, the IP address of Ethernet 1 is 192.168.4.235 with a subnetmask of 255.255.255.000 and the network's default gateway is 192.168.4.1. These addresses are set in the Network Setup menu.

Next, create a private network in Network and Services > Networks menu of 192.168.5.000 with a subnetmask of 255.255.255.000; give it an arbitrary yet meaningful name, like dialup or modempool.

Then, masquerade this network to Ethernet 1 using the Network Setup > Masquerading menu by selecting the Network and masquerade it to Ethernet 1 (ehto0) and then click add.

Note: IP addresses assigned to the dial-up users are configured in the User Authentication > Radius Client menu. For this case, the Remote Host IP address field in the Radius Client menu would have to be 192.168.5.1+, that is, the plus means pool and the .1 is the starting host address.



Network Setup > SNAT

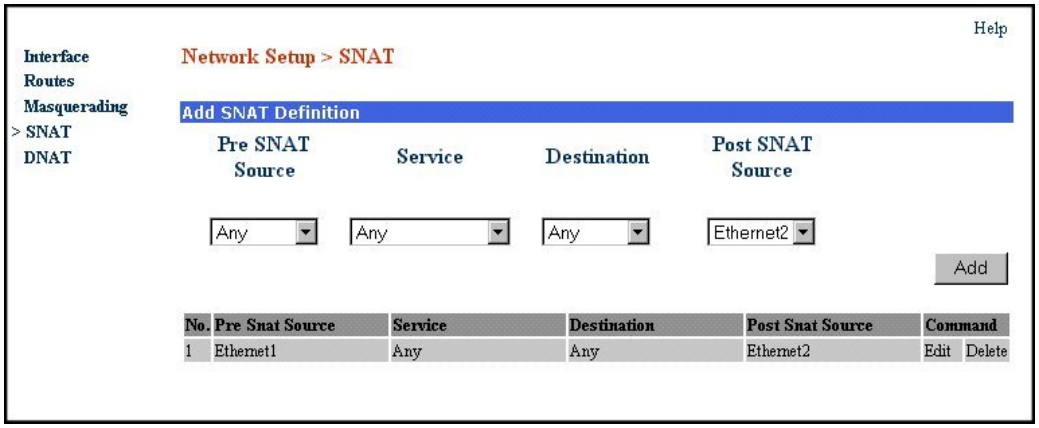
The SNAT (Source Network Address Translation) process allows attaching private networks to public networks. SNAT is used when you want to have a private IP network connected to the Internet via the MultiAccess, since the private IP addresses are not routed on the Internet, you have to apply SNAT on the MultiAccess's public interface.

The MultiAccess's internal interface serves as the default gateway for the LAN. Hence, a rule is added to the firewall to replace the source address of all packets crossing the MultiAccess's external interface from inside to outside with the MultiAccess's own IP address. Once the request gets answered from the Internet host, the firewall will receive the reply packets and will forward them to the client on the LAN.

On this screen you can set up the MultiAccess's ability to rewrite the source address of in-transit data packages using SNAT. This functionality is equivalent to DNAT, except that the source addresses of the IP packets are converted instead of the target addresses being converted. This can be helpful in more complex situations (e.g., diverting reply packets of connections to other networks or hosts).

Important: For SNAT support, the TCP and/or UDP settings must be enabled at **Networks & Services > Services > Protocol**.

Important: As the translation takes place after the filtering by packet filter rules, you must allow connections that concern your SNAT rules in **Packet Filters > Packet Filter Rules** with the original source address. Packet filter rules are covered later in this chapter.



Note: To create simple connections from private networks to the Internet, you should use the **Network Setup > Masquerading** function instead of SNAT. In contrast to Masquerading, SNAT is a static address conversion, and the rewritten source address does not have to be one of the MultiAccess's IP addresses.

Add SNAT Definition

From the drop down list boxes, select IP packet characteristics to be translated. The options are:

Pre SNAT Source

Select the original source network of the packet. The network must be predefined in the **Networks** menu. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Service

Allows the corresponding service for the Pre SNAT Source entry field to be chose from the select menus. The service must have already been defined in the **Services** menu.

Destination

Select the target network of the packet. The network must have been defined in the **Networks** menu. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Post SNAT Source

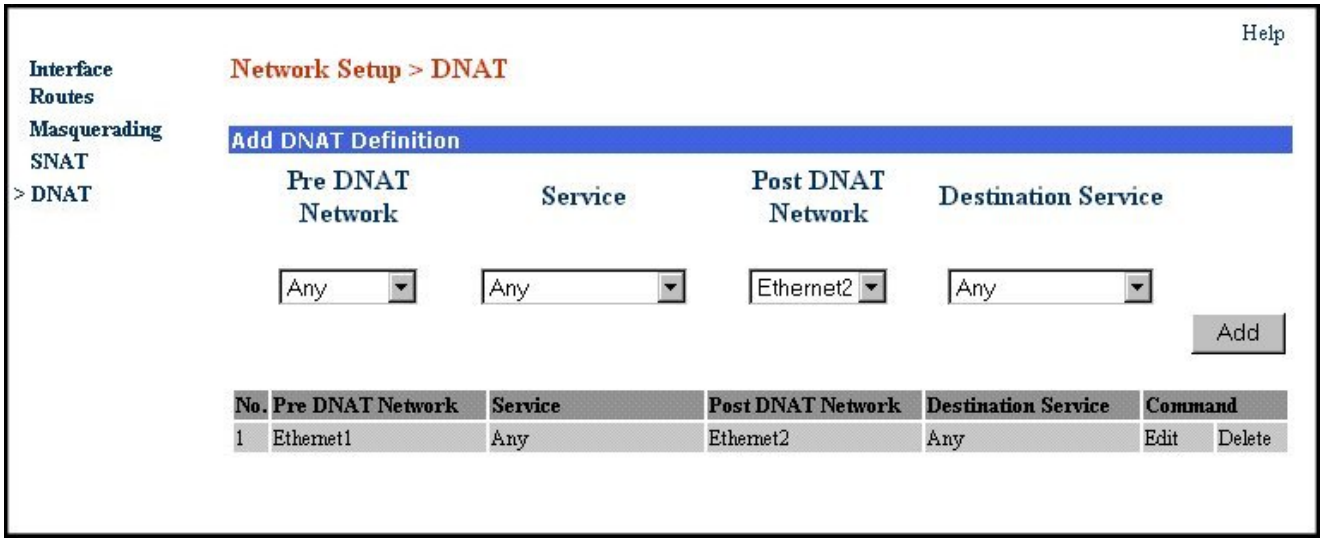
Selects the source addresses of all the packets after the translation. Only one host can be specified here. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Network Setup > DNAT

On this screen you can set up DNAT re-routing. DNAT (Destination Network Address Translation) allows you to place servers within the private network and make them available for a certain service to the public network. Normally the network has a server running on the LAN, providing a network service, with an address in the specified range and wants this service accessible to the outside world. DNAT process running on the MultiAccess translates the Destination address of incoming packets into the address of the real network server on the private network. The packets then get forwarded.

Note that for DNAT support, the TCP and/or UDP settings must be enabled (at **Networks & Services > Services > Protocol**).

Important: You **cannot** add a DNAT rule with the Pre DNAT Network as ANY, with Service as ANY, and a Destination Service as ANY. All the packets will be routed to the system with Post DNAT network, and then the services in the MultiAccess will not function properly.



Add DNAT Definition

The DNAT screen contains four drop down list boxes. The first two define the original target of the IP packets that are to be re-routed. The last two define the new target to which the packets are forwarded. From the drop down list boxes, select IP packet characteristics to be translated.

Pre DNAT Destination

Select the original target host or network of the IP packets that are to be re-routed. The network must be predefined in the Networks menu.

Post DNAT Destination

Select a host to which the IP packets are to be diverted. Only one host can be defined as the Post DNAT destination.

Important: If you are using a port range as the Post DNAT Service, you must enter the same Service definition as you entered in the Pre DNAT Service.

Note: As the address conversion takes place BEFORE the filtering by the packet filter rules, you must set the appropriate **Packet Filter Rules** to let the already translated packets pass. You can find more about setting packet filter rules later in this chapter.

Add, Edit, Delete

Click the **Add** button to save your choices. After saving the settings, a table is created. You can edit or delete entries by highlighting the desired entries and clicking either the **Edit** or **Delete** button listed under ***Command***.

DNAT Example

In this example, your private network is 192.168.0.0/255.255.255.0 and an IP address 192.168.0.20 for the Web server provides accessibility for clients outside your LAN. These clients cannot contact its address directly, as the IP address is not routed in the Internet. It is, however, possible to contact an external address of your MultiAccess from the Internet. With DNAT, you can re-route HTTP Service on the MultiAccess's external interface onto the Web server.

Note: To divert port 443 (HTTPS), you must change the value of the Web Admin TCP port in the Network & Services > Services (e.g., port 444).

Examples of DNAT Network Combinations

You <u>can</u> map:
IP/Port ⇒ IP/Port
IP/Port-Range ⇒ IP/Port
IP/Port-Range ⇒ IP/Port-Range (only if the Port-Range is the same for PRE and POST)
IP-Range/Port ⇒ IP/Port
IP-Range/Port-Range ⇒ IP/Port

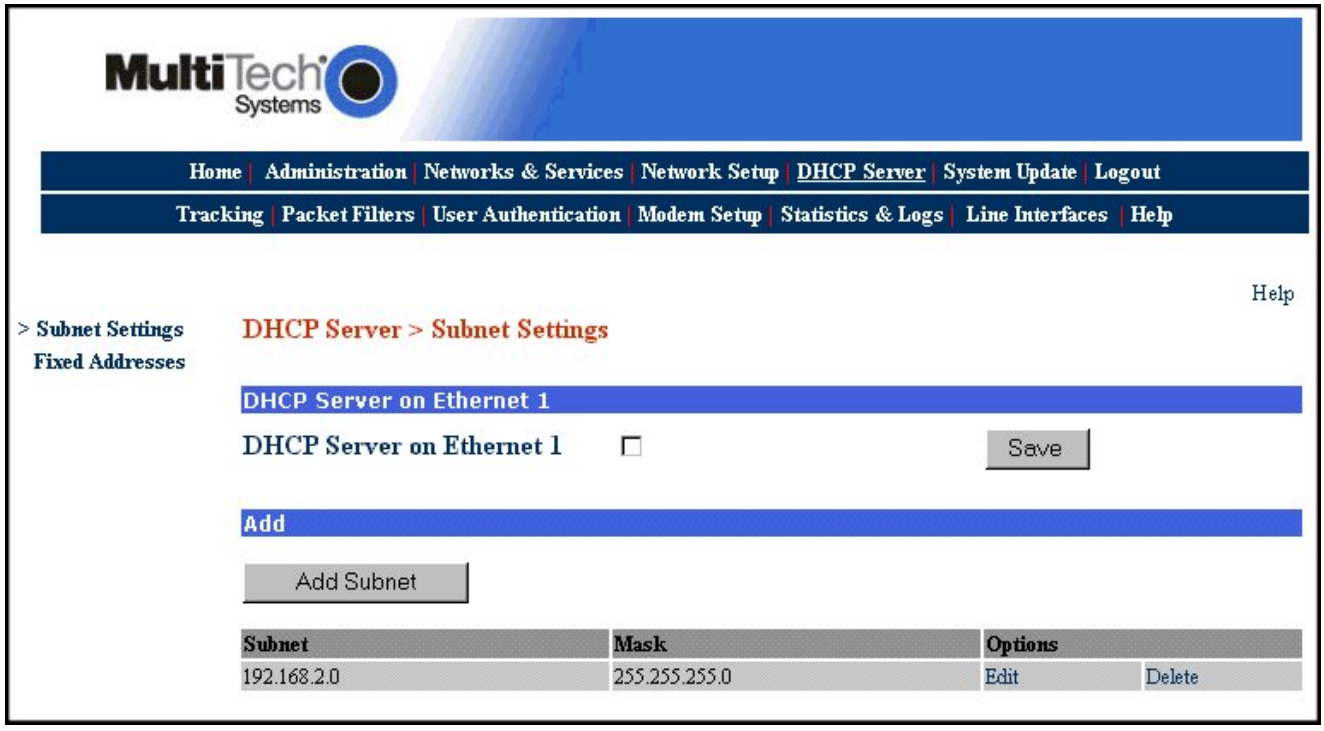
You <u>cannot</u> map:
IP ⇒ IP
IP-Range ⇒ IP
IP-Range ⇒ IP-Range
IP ⇒ IP-Range (load balancing)
The "way back" (return) translation is done automatically; you do not need a rule for it.

Caution: As the address conversion takes place BEFORE the filtering by the packet filter rules, you must set the appropriate rules in the **Packet Filters > Packet Filter Rules >Add User Defined Filters** menu to let the already-translated packets pass. You can find more about setting packet filter rules later in this chapter.

DHCP Server

DHCP Server > Subnet Settings

DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of the DHCP is to make it easier to administer a large network. The DHCP package includes the DHCP server and a DHCP relay agent.



DHCP Server on Ethernet 1

DHCP Server on Ethernet 1

To Enable DHCP Server on Ethernet 1, check the corresponding checkbox. Click the **Save** button to activate the change.

Add

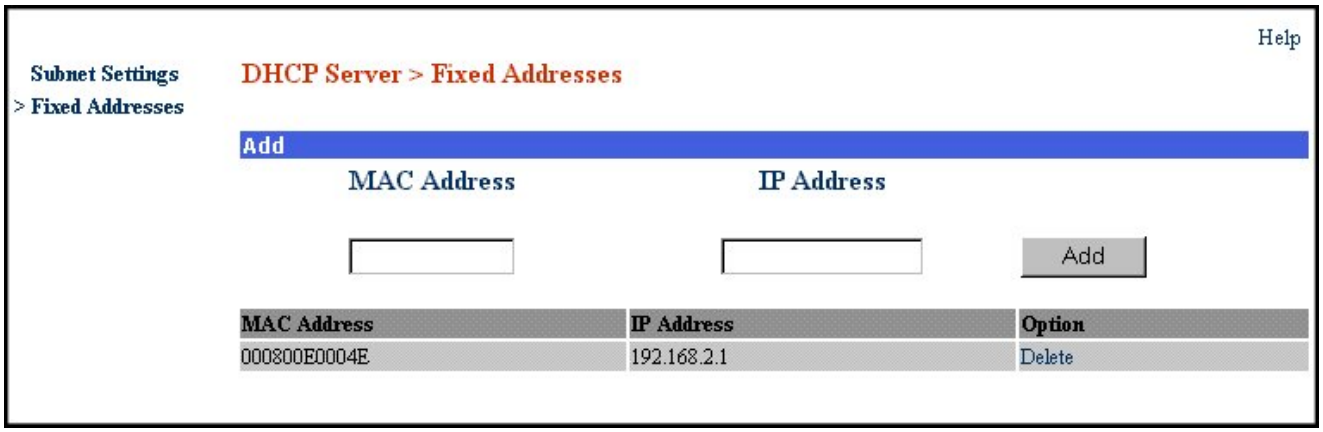
Click the **Add Subnet** button, which will open a screen for entering the Subnet IP Address and Mask.

Edit or Delete

You can edit or delete entries by selecting the desired entries and clicking either the **Edit** button or **Delete** button listed under **Command.**

DHCP Server > Fixed Addresses

The DHCP server can be made to assign a fixed IP address for a particular user by identifying the MAC address. This binding can be made permanent by configuring the same using this screen. The same IP address would not be used for any DHCP client with a different MAC address, even if there were no active DHCP connection with that IP address.



DHCP Server Fixed Addresses

Add

Enter both a MAC address and an IP address.

Option

Edit or Delete

You can edit or delete entries by highlighting the desired entries and clicking either the **Edit** button or **Delete** button listed under **Command**.

System Update > Available

When you select System Update from the main menu bar, you are brought to the "Available" screen. This screen invokes the MultiAccess "update client", which checks for "Available" updates. The update client checks by opening an FTP connection to the host defined on the "Setup" screen. The default update server is a server at Multi-Tech Systems (update.multitech.com). If the update client is successful in communicating with the update server, and a newer version is available, it will display a summary of changes per version and allow you to apply it.

MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
> Available
Applied
Setup
System Update > Available
Available Updates
The update server was contacted but a newer version is not available. Version 1.14 is the latest version.

When you select "apply" (including popup to confirm), you will be logged out of the current HTTPS administration session and be brought back to a login menu. The login menu will reflect the version being updated to, however at this point it is just a cosmetic indication. You must wait for the update process to complete before you can log back in.

When you apply the update; the update client downloads the compressed update file or files (*version*.tar.gz) from the update server, extracts to a temporary location, backs up the corresponding old files, copies in the new files and then reboots the MultiAccess. Depending on the how many updates are being applied and the contents of the updates, you may be able to log back in - in as quickly as 2 minutes (or you may have to wait longer - like in the case of updating from version 1.09 to 1.10 it takes appx 30 minutes). Most updates take 2 or 3 minutes. Some updates may include a process that does not start until the unit is booting up, which increases the time it takes to complete. It can be helpful to attach a video monitor to the back of the MultiAccess when applying updates.

If there is not correct FTP communication between your MultiAccess and the defined Update Server, you will see the following message:

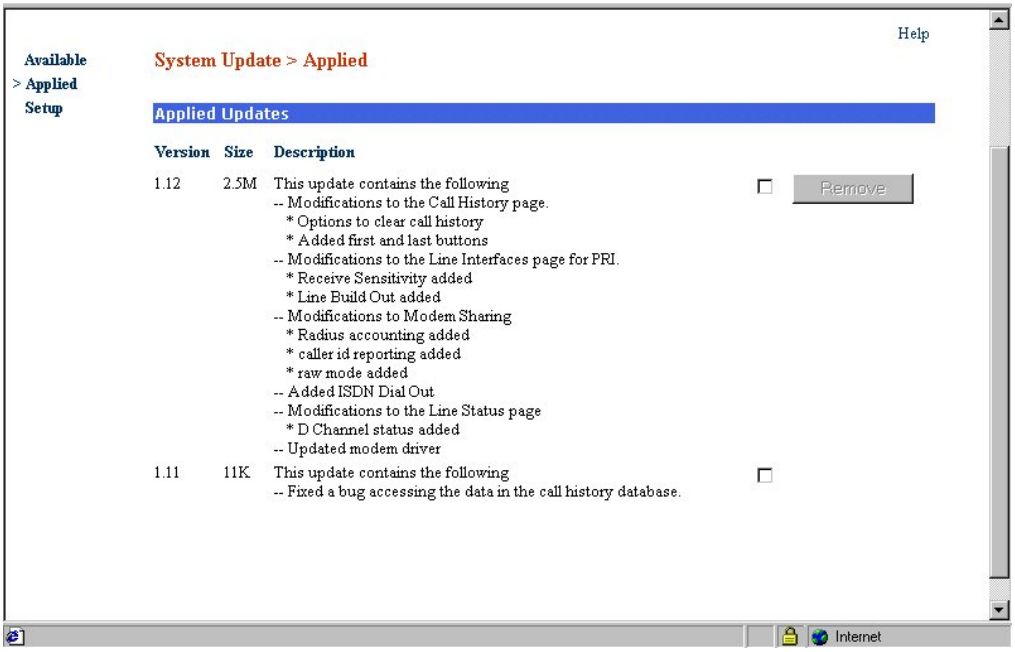
There was a problem connecting to the ftp server. Please make sure the following items are set correctly:

- The update server is correctly defined on the Setup page.
- The default gateway is correctly defined on the Network Setup page.
- The DNS address is correctly defined on the Network Setup page.
- If the MultiAccess is on a private network, the IP addressed assigned to the MultiAccess is routable to the Internet and not blocked by your firewall.

If the update client was able to communicate with the update server, but your unit is already at the latest version you will see the message:
"The update server was contacted but a newer version is not available. Version#.## is the latest version."

Applied

This menu lists updates that have been applied to the unit since it's hard drive image was created. This menu also provides the ability to remove updates. The screen shot below indicates this unit's original version was 1.10 and that version 1.11 and 1.12 have been applied to it.


Help
Available
> Applied
Setup
System Update > Applied
Applied Updates
Version Size Description
1.12 2.5M This update contains the following
-- Modifications to the Call History page.
* Options to clear call history
* Added first and last buttons
-- Modifications to the Line Interfaces page for PRI.
* Receive Sensitivity added
* Line Build Out added
-- Modifications to Modem Sharing
* Radius accounting added
* caller id reporting added
* raw mode added
-- Added ISDN Dial Out
-- Modifications to the Line Status page
* D Channel status added
-- Updated modem driver
Remove
1.11 11K This update contains the following
-- Fixed a bug accessing the data in the call history database.
Internet

Setup

The Setup menu allows for the administrator to define the location of the update server. This would be necessary in situations were network security is foremost.

MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Available
Applied
> Setup
System Update > Setup
Update Server Setup
Update Server
update.multitech.com
Save

The administrator would most likely use a separate workstation to manually down load the appropriate update files from update.multitech.com, and then put them on a private internal FTP server. Appropriate files are defined as a version.tar.gz and a version.html file per MA30120 version.

The IP address or DNS resolvable internal name of this private FTP server would be defined in the Update Server field. The update files must be placed in the correct/default directory of the FTP server.

The Update Server field is limited to a host address (do not specify a sub directory on the FTP server). The Update Client can not instruct the FTP session to change directories on the FTP server. The FTP server must allow binary file transfer.

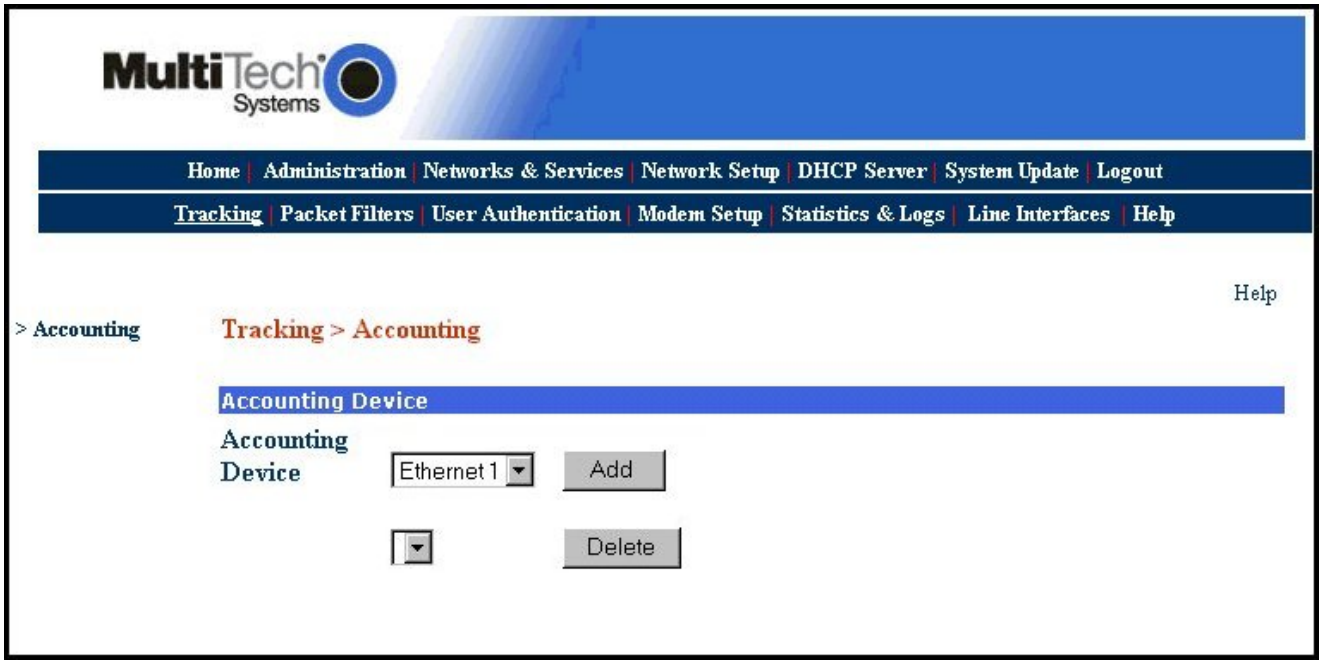
Note: The Update Client in the MultiAccess uses anonymous credentials when logging into the Multi-Tech Update server and when logging into a user define update server.

Tracking

Tracking > Accounting

The Accounting function records all the IP packets through the network cards and sums up their size. The traffic sum for each day is calculated once a day. Additionally, the traffic sum for the current month is calculated and displayed. This is the amount that your ISP (Internet Service Provider) will charge to you if your payment plan is based on the amount of data you transfer.

On this screen you can specify which local devices will have their network traffic counted and recorded. You can also exclude hosts or networks from the accounting process.
After this accounting is in place, you can view the Accounting of your MultiAccess in the **Statistics & Logs > Accounting** menu.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
> Accounting
Tracking > Accounting
Accounting Device
Accounting Device
Ethernet 1
Add
Delete

Accounting Device

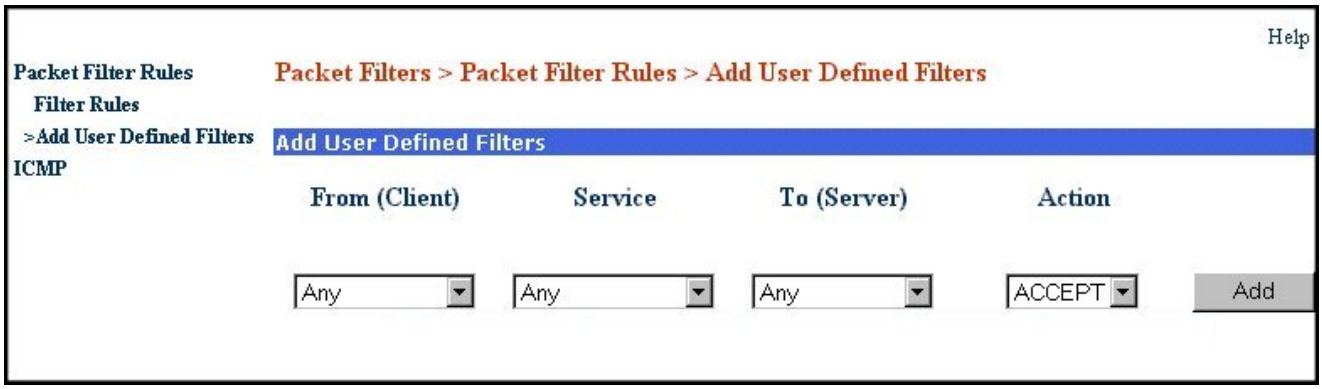
Accounting Device

From the Accounting Device drop down box, select the network to have its traffic counted. The options are **Ethernet 1** and **Ethernet 2**. Click the **Add** button to confirm your entry. After the entry is activated, a window for this network is created. You can delete an entry in this window by highlighting the desired entry and clicking the **Delete** button.

Packet Filters

Packet Filter Rules > Add User Defined Filters

The Packet Filter is a key element of the MultiAccess. Packet Filter Rules define the type of data traffic allowed between networks and hosts. You can specify whether particular packets are to be passed through the system or filtered. The rules are created with the help of the definitions you set up previously in the **Networks & Services** section of this software.



See the ICMP menu (accessed from the left side of this screen) in which you can switch on the ICMP forwarding between networks, as well as the ICMP (e.g., **ping**) reception for the MultiAccess itself.
To display rule violations and see an overview of the entire rule setup (packet filter, NAT), access the Filter LiveLog.

Packet Filter Rules > Filter Rules

When you click the **Filter Rules** button, a screen of system rules displays.

Generally speaking “everything that is not explicitly allowed is forbidden”.

The MultiAccess’s behavior is determined by the content and order of the filter rules. The filter rules are assigned by column number (column **No**). Every incoming data packet is checked, in order, as to whether rule 1 is valid; rule 2 is valid, etc.) As soon as a correspondence is found, the procedure as determined by the action is carried out. You can **Accept**, **Drop, Reject, and Log** the packets. When packets are denied (**Rejected** setting) an entry in the appropriate log-file occurs.

All rules are entered according to the principle: **From Client** - **Service** - **To Server** - **Action**.

To be able to differentiate rules, the appropriate **Networks & Services > Service Groups** and **Networks & Services > Network Groups** must first be defined.

When setting packet filters, the two fundamental types of security policies are:

- All packets are allowed through – **Rules Setup** has to be informed explicitly what is forbidden.
- All packets are blocked – **Rules Setup** needs information about which packets to let through.

Your MultiAccess default is that all packets are blocked **setting**, as this procedure can achieve an inherently higher security. This means that you explicitly define which packets may pass through the filter. All other packets are blocked and are displayed in the Filter LiveLog.

Example: Network A is contained in network B.
Rule 1 allows network A to use the SMTP service.
Rule 2 forbids network B to use SMPT.
Result: Only network A is allowed SMPT.
SMPT packets from all other network B IP addresses are not allowed to pass and are logged.

Caution: Re-sorting the rules may change how the MultiAccess operates. Be very careful when defining the rule set. It determines the security of your MultiAccess.

Caution: If one rule applies, the subsequent ones are ignored. Therefore, the sequence is very important. **Never** place a rule with the entries **Any – Any – Any – Accept** at the top of your rule set, as such a setting will match all packets, and thus, cause all subsequent rules to be ignored.

Add User Defined Packet Filter Rules

Choosing from four drop-down lists creates new packet filter rules. All services, networks, and groups previously created in Definitions are presented for selection. In Edit rule, use the **Save** button to create the appropriate rule as a new line at the bottom of the table. The status of the new rule is initially inactive (red dot next to it), and can be manually activated afterwards. The new rule automatically receives the next available number in the table. The overall effectiveness of the rule is decided by its position in the table. You can move the new rule within the table with the **Move** function in the **Command** column.

From Client: Select the network from which the information packet must be sent for the rule to match. You can also select network groups. The Any option can also be given which matches all IP addresses, regardless of whether they are officially assigned addresses or so-called private addresses. These Network clients or groups must be pre-defined in the Networks menu.
Example: net1 or host1 or Any

Service: Select the service that is to be matched with the rule. These services are pre-defined in the Services menu. With the help of these services, the information traffic to be filtered can be precisely defined. The default entry Any selects all combinations of protocols and parameters (e.g., ports).
Example: SMTP, ANY

To Server: Select the network to which the data packets are sent for the rule to match. Network groups can also be selected. These network clients or groups must be pre-defined in the Networks menu.

Action: Select the action that is to be performed in the case of a successful matching (applicable filter rule). There are three types of actions:

- **Accept:** This allows/accepts all packets that match this rule.
- **Reject:** This blocs all packets that match this rule. The host sending the packet will be informed that the packet has been rejected.
- **Drop:** This drops all packets that match this rule, but the host is not informed. The action Drop is recommended for filter violations that constantly take place, are not security relevant, and only flood the LiveLog with meaningless messages (e.g., NETBIOS-Broadcasts from Windows computers).

  To drop packets with the target address Broadcast IP, you first have to define the appropriate broadcast address in the form of a new network in the Networks menu (defining new networks is explained in detail earlier in this chapter). You must then set and enable the packet filter rule.

To Broadcast on the Whole Internet:

1. Open the Networks menu in the Definitions directory and enter the following data:
   Name: **Broadcast32**
   IP Address: **255.255.255.255**
   Subnet Mask: **255.255.255.255**
2. Confirm your entries by clicking the Add button.
3. Open the Rules menu in the Packet Filter directory and set the packet filter rules:
   From (Client): Any
   Service: Any
   To (Server): Broadcast32
   Action: Drop
4. Confirm your entries by clicking the Add button.

To Broadcast on One Network Segment

1. Open the Networks menu in the Definitions directory. Enter the following data into the entry fields:
   Name: **Broadcast8**
   IP Address: 192.168.0.255
   Subnet Mask: **255.255.255.255**
2. Confirm your entries by clicking the Add button.
3. Open the Rules menu in the Packet Filter directory and set the packet filter rules:
   From (Client): Any
   Service: Any
   To (Server): Broadcast8
   Action: Drop
4. Confirm your entries by clicking the Add button.

- **Log:** The packets matching the corresponding source address, destination address, service will be logged. The log messages can be viewed from the Statistics&Logs >Packet Filter >Packet Filter Livelog screen.

Add: Confirm your entry by clicking the **Add** button. After a successful definition, the rule is always added to the end of the rule set table. Entries can be edited by clicking the **Edit** button, which loads the data into the entry menu. The entries can then be edited. The changes are saved by clicking the **Save** button.

Delete: Rules can be deleted by clicking the **Delete** button.

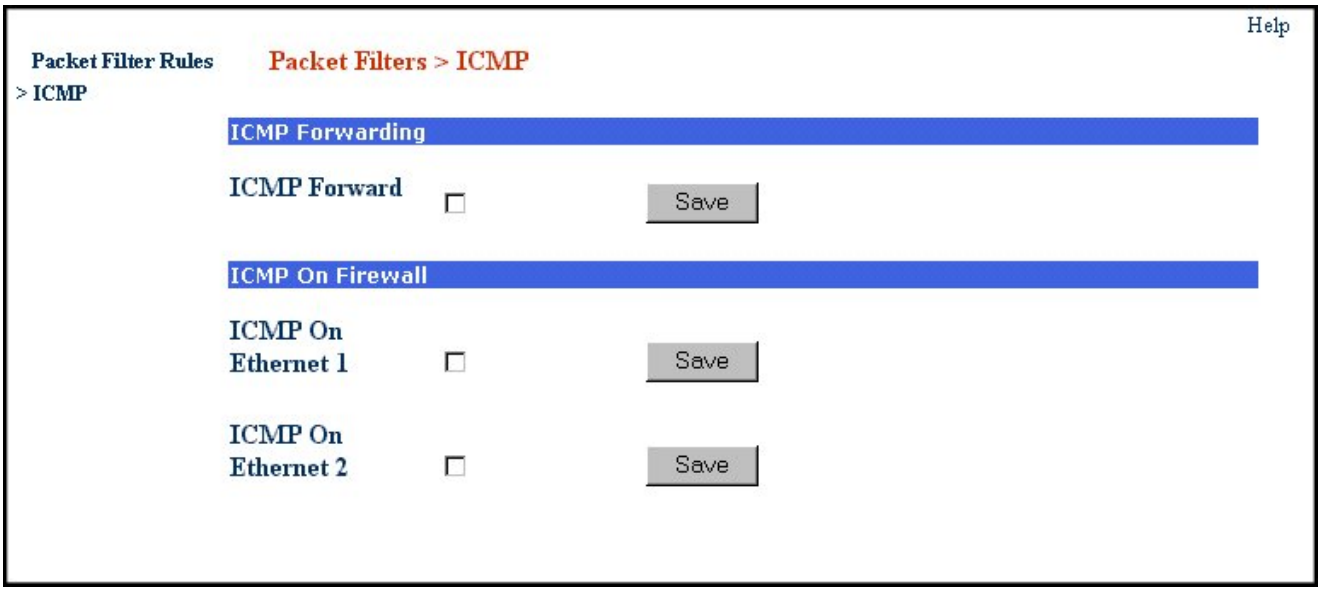
Important:

- The order of the rules in the table is essential for the correct functioning of the firewall. By clicking the **Move** button, the order of execution can be changed. In front of rule to be moved, enter the line number that indicates where the rule should be placed. Confirm by clicking **OK**.
- By default, new rules are created at the end of the table in the inactive state. The rule only becomes effective if you assign the active state.

Packet Filters > ICMP

ICMP (Internet Control Message Protocol) is necessary to test network connections and to test functionality of your firewall.

ICMP-forwarding and ICMP-on-firewall always apply to all IP addresses (“Any”). When these are enabled, all IPs can ping the firewall (ICMP-on-firewall) or the network behind it (ICMP-forwarding). Separate IP addresses can then no longer be ruled out with packet filter rules. If the ICMP settings are disabled, separate IPs and networks can be allowed to send ICMP packets through the firewall by using appropriate packet filter rules.



ICMP Forwarding

Check the ICMP Forward checkbox to enable the forwarding of **ICMP** packets through the MultiAccess into the local network and all connected DMZs. In this way you select whether an ICMP packet should be dropped or passed through to the local network and all connected DMZs.

If **ICMP forward** is enabled, ICMP packets go through all connected networks. Another use of ICMP forwarding is to allow ICMP packets to be forwarded to individual networks (set in **Packet Filter > Rules**). For this, **ICMP forward** in **Packet Filter > ICMP** must be disabled.

The status is activated by clicking the Save button.

ICMP on Firewall

Check the ICMP on Ethernet 1 or Ethernet 2 checkbox to enable the direct sending and receiving of **ICMP** packets by the MultiAccess.

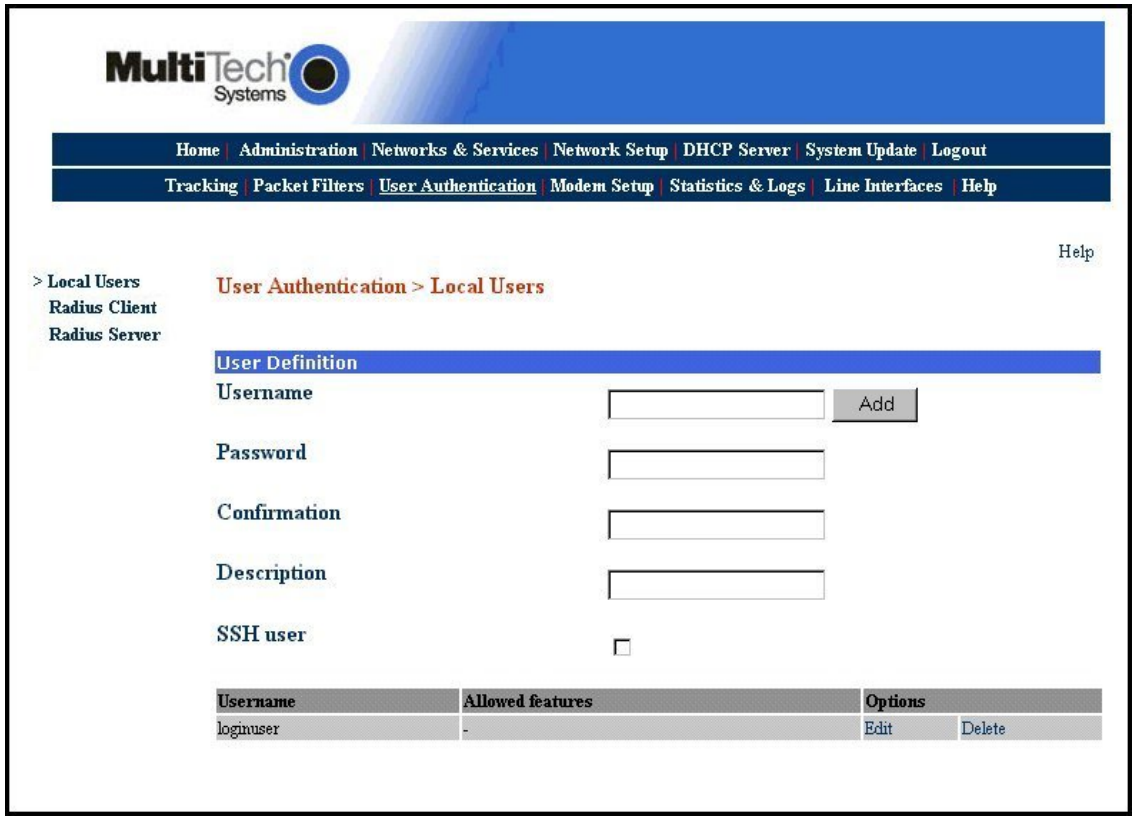
The status is activated by clicking the Save button.

User Authentication

User Authentication consists of three menus, Local Users, Radius Client, and Radius Server. These menus are used to define user credentials (user name and passwords), and database access details (client/server locations, etc).

User Authentication > Local Users

User's added to this data base can access the MultiAccess via command shell (limited to user level access rights). They also, have rights to use modems configured for Modem Sharing with Local Authenication.



User Definition

User Name

Limited to alphanumeric characters with at least one letter. A user name of all numbers is not supported. Maximum user name is 30 characters. User name is case sensitive.

Password

The password is limited to alphanumeric characters with a maximum of 8 characters. Password is case sensitive.

Confirmation

Confirm the password entered above by entering it again.

Description

Enter a short comment that will identify the user to you.

SSH User

Check this checkbox if you want the user to have SSH access.

Add Button

Click the **Add** button after all the parameters are entered. After a successful definition, the new user is entered into the user table.

Edit or Delete

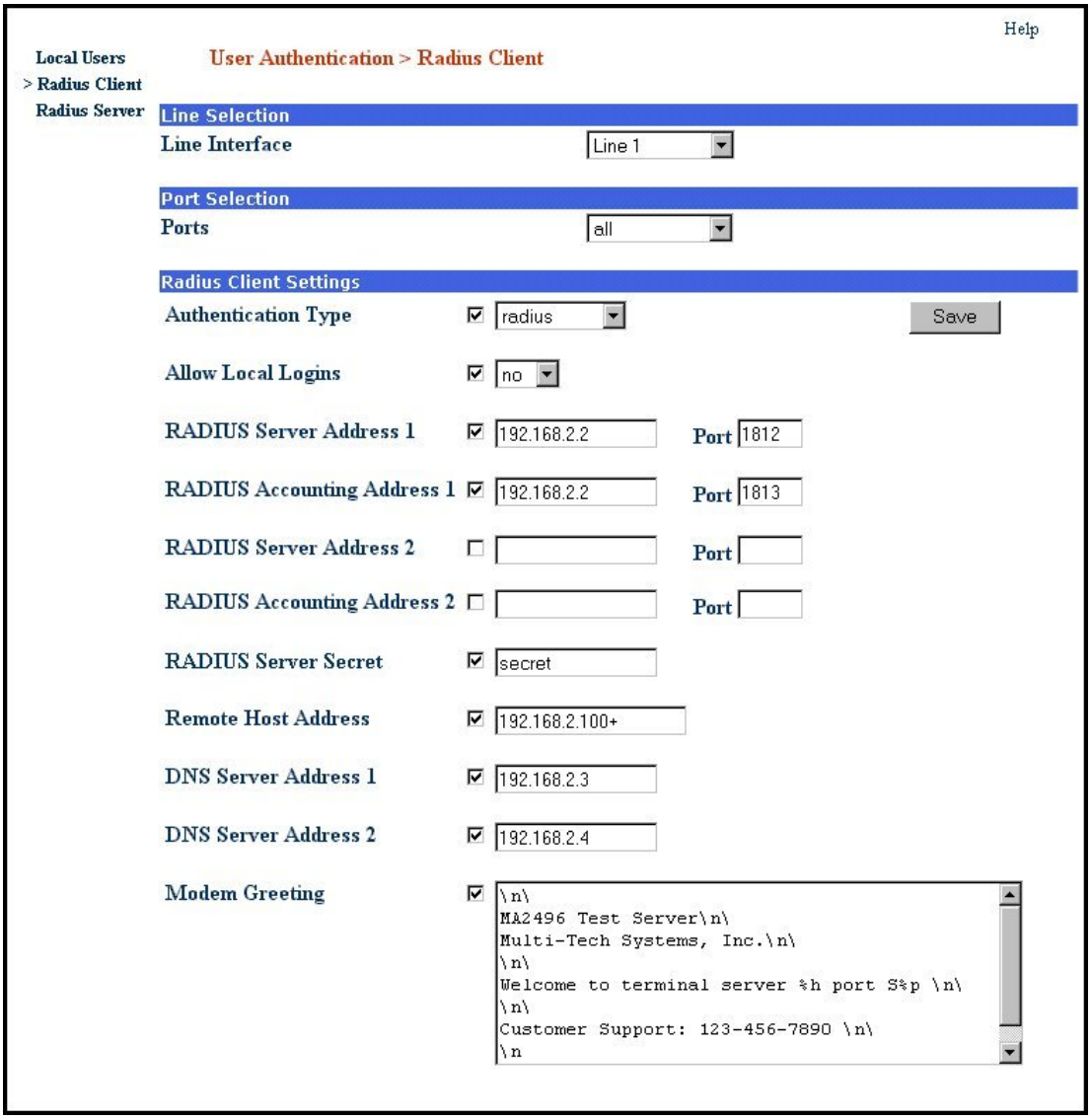
You can edit or delete entries in the table by clicking on either the **Edit** button or **Delete** button listed under **Options**.

User Authentication > RADIUS Client

The RADIUS client menu must be used when the a modem's usage is setup for RAS or Modem Sharing with RADIUS Authentication.

The Radius Client is responsible for making authentication requests to the Radius server and then acting upon the response from the Radius server. The Radius Client screen allows you to select which Digital Line Interface and ports are to be used. This screen also defines the dynamic IP address pool and related parameters synomomous with traditional PPP remote access environments.

Note: The RADIUS protocol (RFCs 2138 & 2139) implements a client\server relationship. RADIUS software uses UDP (of TCP/IP) to communicate between client and server. The MultiAccess contains both RADIUS Client and RADIUS Server software. These are separate entities within the System. The RADIUS client in the MultiAccess can be a client to an external RADIUS server (already running on your network). This means you do NOT have to enable and use the internal RADIUS server. However, the MultiAccess RADIUS Client can be a client to both internal and external servers.



Radius Client Settings

When you first enter the Radius Client settings, you first have to identify the line interface and ports accessible to Radius.

Authentication Type
This option tictates the authorization process performed by the Radius Client. You can choose the Authentication Type by clicking on the down arrow and choosing from none or radius (the default). None accepts all request with no security. Radius sends the user crentials to the defined Radius Server for authorization processing. The other options (tacacs, remote, local and radius/local) listed are not functional at this time.

Allow Local Logins
The default is No. Setting this to yes allows command shell access to the system with user level access rights. To achieve this command shell access, the account credentials provided must be that of a local user and when entered at the time of connecting/authenticating, it must begin with a "!" (exclamation point). For example, at the Local User's menu, add the account user name of "troberts" with a password of "58Xz21A". Then dial-in, at the login prompt enter "!troberts" as the username and a password of "58Xz21A". The Radius Client will strip off the ! and run the credentials against the Local Data base.

Caution: If you change this to yes and put a"!" before the login name, you could be setting up a potential security risk. You can use this in an **emergency situation** if your radius server goes down.

RADIUS Server Address 1
The RADIUS Server Address 1 points the client to the primary Radius Server. Enter the IP address of your primary Radius Server in this window.
Port
The top Port window is the UDP port number that the client communictes with the main Radius Server.

RADIUS Accounting Address 1
Radius Accounting host keeps track of information such as login time, logout time, port number, etc. This is the IP address of your primary Radius Accounting host.
Port
The next Port window down is the UDP port number used to communicate with the main Radius Accounting host.
RADIUS Server Address 2
RADIUS Server Address 2 is used when a back up or secondary Radius Server is used in your network. Click on the check mark window and enter the IP address of the secondary or back up Radius Server. If a secondary or back up server is configured, the primary server is tried five times before switching to the secondary server. They alternate back and forth up to a maximum of 30 times in increments of three seconds per query.
Port
Enter the port number of the secondary or back up Radius Server in the third Port number window.
RADIUS Accounting Address 2
RADIUS Accounting Address 2 is used when secondary or back up Radius Accounting host is used in your network. Click on the check mark window and enter the IP address of the secondary or back up Radius Accounting Server. If a secondary or back up host is configured, the primary host is tried five times before switching to the secondary host. They alternate back and forth up to a maximum of 30 times in increments of three seconds per query.
Port
Enter the port number of the secondary or back up Radius Accounting host in the last Port number window.
RADIUS Server Secret
This is the server secret of the Radius Server. MD5 is the standard Radius encryption technique supported by the MultiAccess. The Radius Server Secret is used for both Address 1 and Address 2. The server secret is limited to alphanumeric characters (a-z & 0-9) and is case sensitive.

Remote Host Address
Remote Host Address is an address pool that is assigned to dial in users. Click on the check mark window and enter the starting IP address of your pool. The IP address needs to have a + (plus symbol) after the number (e.g., 192.168.1.150+). The plus symbol instructs the “portslave” to create an address pool starting with the address you have entered. Portslave determines the “ending” address number by adding up all the Line Interface selections that have their “Port Selection” set to “All”. If the MultiAccess server has multiple line interface modules and all ports are to use an address pool, set this field to the same address (192.168.1.150+) for each line interface.

DNS Server Address 1
This is the IP address of the primary name server. This identifies the name server for remote access users. Click on the check mark window and enter the IP address of the main DNS server.

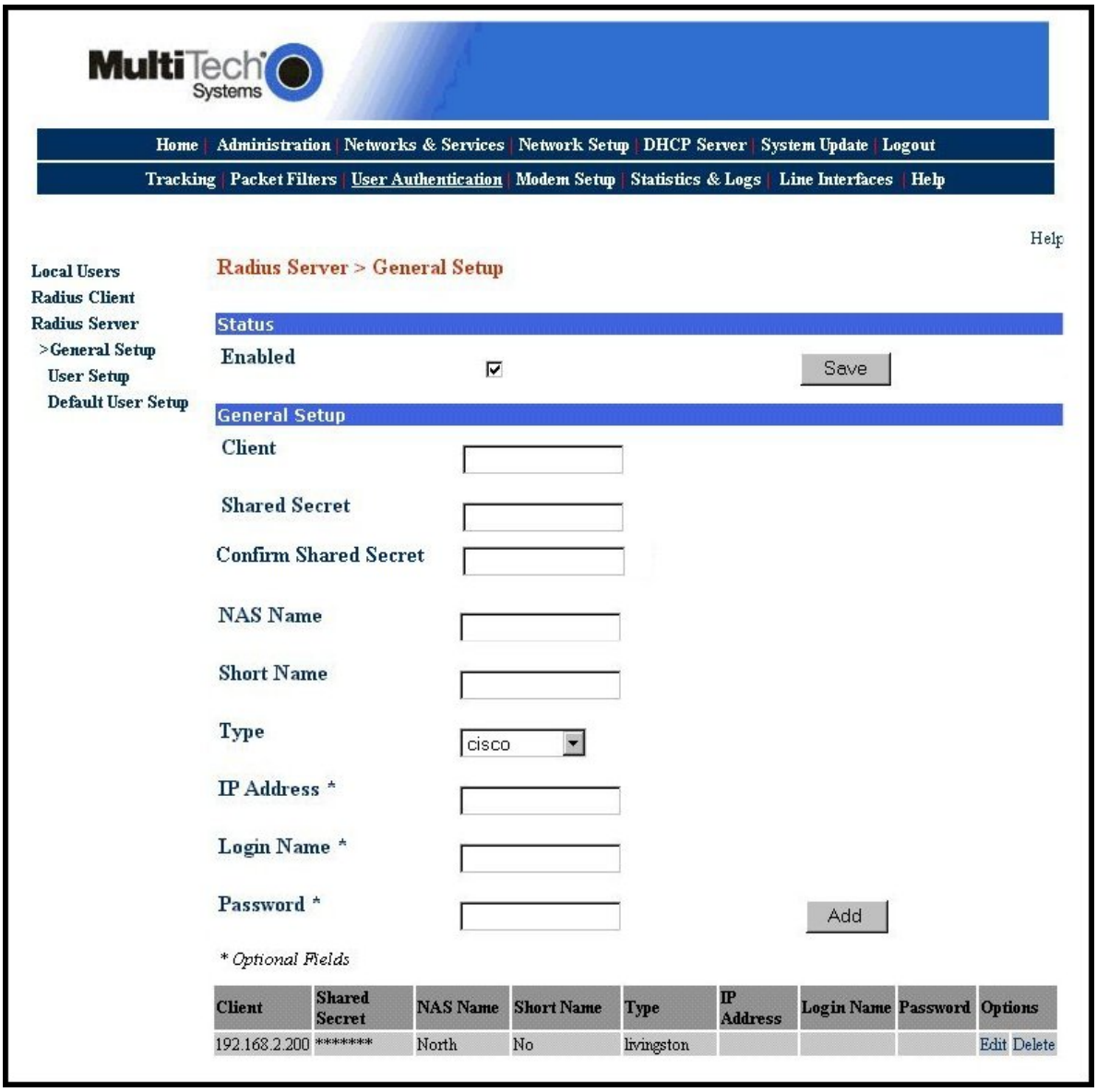
DNS Server Address 2
If a secondary or back up DNS server is used in your network, click on the check mark window and enter the IP address of the secondary or back up DNS server.

Modem Greeting
The modem greeting is sent to the remote user upon connection. If you want to customize the modem greeting you can edit the greeting.

User Authentication > RADIUS Server > General Setup

RADIUS (**Remote Authentication Dial-In User Service)** is a protocol responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. The Radius Server menu consists of three screens, General Setup, User Setup and Default User Setup.

The intended purpose of the MultiAccess's RADIUS Server is for use with the MultiAcces's RADIUS Client. This RADIUS Server can serve the internal Radius Client or MultiAccess RADIUS Clients external to this unit (other MultiAccess units). This RADIUS Server uses (serves) Ethernet 1. The IP address of Ethernet 1 is the IP address of this RADIUS Server.



Note: When the RADIUS Server and RADIUS Client are in the same unit\server, the IP Address for each must be that of Ethernet 1 (eth0).

- The General Setup Screen is used to add RADIUS clients to this server.
- The User Setup Screen is used to create a RADIUS user database.
- The Default User Setup screen is used to define common parameters to all RADIUS users.

The RADIUS protocol implements a client to server relationship. The server is most commonly software running on a network computer (server or workstation), i.e. IAS service on Windows 2003 or Free RADIUS running on Linux. The client is most commonly a communication appliance on the network (such as a remote access server or VPN gateway). RADIUS uses the TCP/IP protocol UDP to communicate between client and server. The RADIUS Client must be told (configured with) the address of the RADIUS Server and the shared secret (password) it is to use. In turn the RADIUS Server is configured with a list of valid clients (listed in the server's "clients" file) with the associated shared secret password.

When the client sends an authentication request, it encrypts the user's password with an encryption key referred to as the "shared secret". The standard encryption technique used by RADIUS is MD5. When the server receives the authentication request, it determines the source address of who sent the request packet, and checks to see if the source is listed in it's clients file, if so, it continues processing and un-encrypts the user's password using the same shared secret (if the sender is not listed, the packet is ignored and the client will not receive any response from the server). The authentication request contains the user's credentials (advanced implementations may contain addititonal identifying attributes like callerID information). The server compares the contents of the request against a pre-defined user entry contained in the server's "user" file (or RADIUS database). The server then replies back with an "accept" or "reject" packet (based on the comparison). The RADIUS client acts accordingly upon receipt of the auth-accept or auth-reject packet. There are variables to what the client may do upon receipt of a reject. When the server sends an accept packet, it will include a list of attributes that should be applied to the user (like the type of user is Framed PPP, the IP Address to use, how long to allow the connection, etc). Upon receipt of an acceptance packet, the client will compare the contents against the current conditions, apply\provide any necessary parameters to the user and allow the connection to proceed. The RADIUS Client at this time (if configured to do so) starts the RADIUS Accounting process. The client then sends an Accounting-Start packet (containing a summary of the user, including resources used, i.e. starting time & date, type of user, port number, IP address, etc) to the RADIUS Accounting Server. When the user disconnects, the RADIUS Client sends an Accounting-Stop packet to the accounting server (which includes a summary similar to the start packet). The RADIUS server will send an acknowledgment to the client for each accounting packet received from the client.

Note: The MultiAccess RADIUS Server also has the ability to queary the Linux system local database. Accounting is always on in the MultiAccess Client.

Radius Server General Setup

The general setup will set the conditions for the Radius Server within the MultiAccess to be used. If you already have a Radius Server on your network, you do not need to configure the Radius Server in MultiAccess.

Status

Click on the check mark window to enable the Radius Server. Click on the Save button to activate the Radius Server.

Client

This is the IP address of the Radius Client. This field points the Radius Server to the Radius Client. You need one client entry for each Network Access Server (NAS). If the client is an internal Radius Client, then the IP address must be that of Ethernet 1 (eht0).

Shared Secret

The Shared Secret is the encryption key used by Radius to encrypt and unencrypt the user's password for security reasons when sending the Auth request across the network. MD5 is the standard Radius encryption technique supported by the MultiAccess. This shared secret is used by the client in requests to this server. The shared secret is limited to 15 alphanumeric characters (a-z & 0-9) and is case sensitive.

Confirm shared Secret

Confirm the shared secret entered above by entering it again.

NAS Name

Network Access Server (NAS) Name is an meaningful arbitrary name, such as North in the screen above that is unique for each NAS.

Short Name

This is a meaningful arbitray Short Name for NAS name that is used for creating a directory for the location of the accounting detail file for this client.

Type

Type is the manufacture of the Radius client, such as MultiTech, Livingston, etc. Click on the drop down arrow and high light the manufacture of the Radius Client (NAS).

IP Address*/Login Name*/Password*

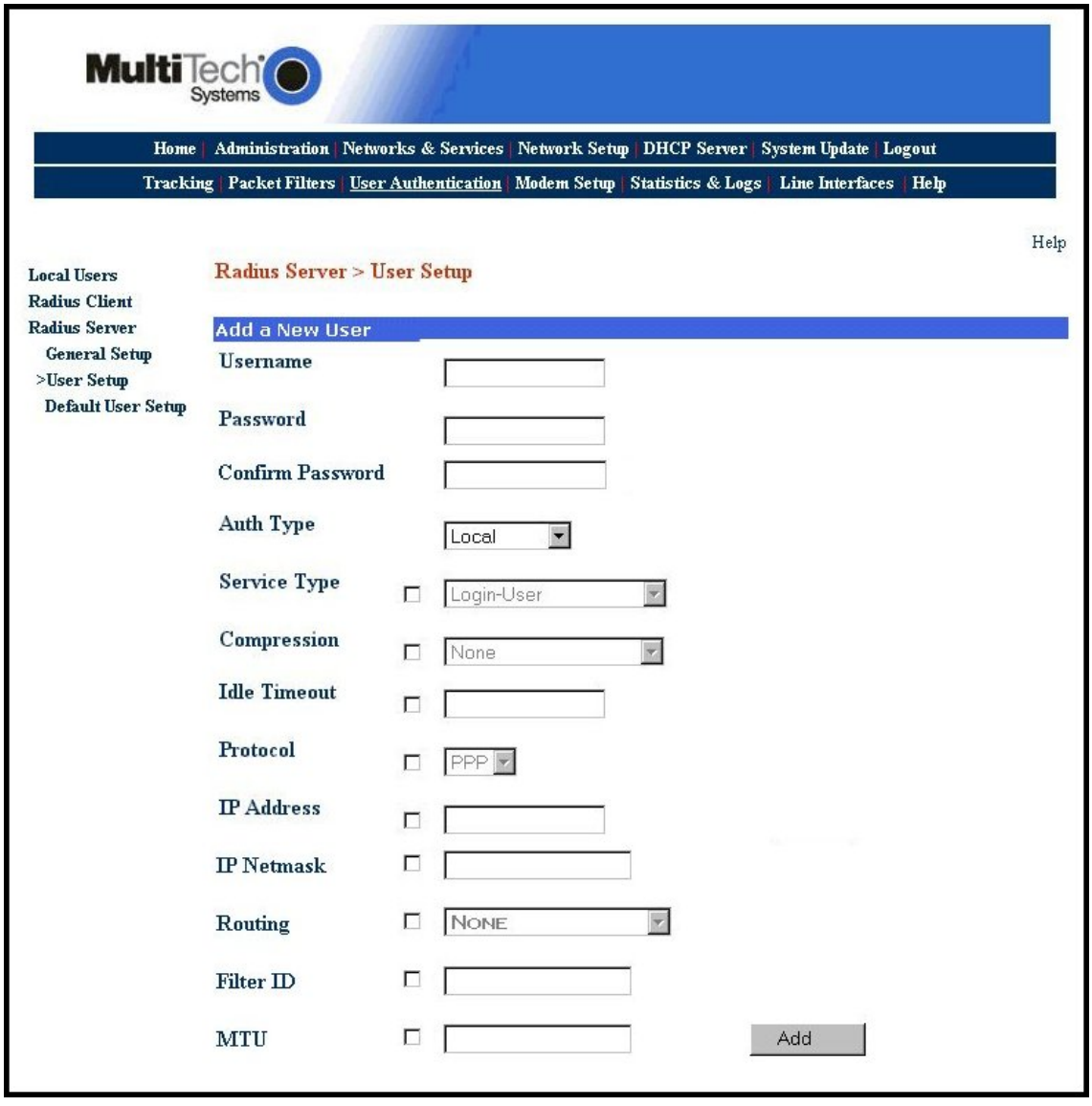
All three optional and currently not used.

Add

Click the Add button to configure the Radius Server with the MultiAccess and the above client information.

User Authentication > RADIUS Server > User Setup

This menu establishes a RADIUS User database within the MultiAccess. These users will have rights to use the modems configured for Modem Sharing with RADIUS Authentication and the modems configured for RAS. Internally, these user accounts are contained in a file called “users”. This file is considered “local” to the RADIUS server - however this reference and these user accounts are separate for the Local Users of the MultiAccess Linux Operating System. The RADIUS Server will check it’s local users file first, and if a match of username and password is not found, it will proceed to check the Local Users of the Linux system.



Add Users

Username

Up to 15 alphanumeric characters, case sensitive, can be used with the exception of four capitol letters (C, P, S & U). The four capitol letters can not be used as the 1st letter of a user name. Doing so results in authentication failure.

Password

This is the password that the remote user will use. The password can have as many as 15 alphanumeric characters and is case sensitive.

Confirm Password
Confirm the password entered above by entering it again.

Auth Type
This field defines where the Radius Server is to look for the user's credentials and dictates the format of how the password is stored. The default value is "Local" and currently this is the only option supported. Local means the value of Password is clear text.

If you check one of the following User attributes, it will over ride the default value defined in the Default User Setup menu.

Service Type

This field indicates the type of service the user is to be provided. Values of "framed" or "outbound" are supported.

Compression

This field indicates if Van Jacobson IP compression is to be allowed (applies to Framed protocol PPP).

Idle Timeout

This field indicates to the NAS equipment how long the user can be idle in seconds while connected, applies to Framed protocol PPP.

Protocol

This field indicates the type of framed service the user is to be provided.

IP Address

This field indicates the IP address the framed user is to use. A value of 255.255.255.255.254 instructs the NAS equipment to give the user an IP address from an address pool defined within the NAS equipment, referred to as a dynamic IP address. A value of 255.255.255.255 instructs the NAS equipment to let the user pick it's own IP address. A unique specific value can also be defined, i.e., 206.37.212.39, referred to as a static IP address.

IP Netmask

This field indicates the subnet mask that should be applied to this connection.

Routing

This field indicates the routing function for when the user is a router.

Filter ID

This field indicates to the NAS the filter policy that should be applied to this connection.

MTU

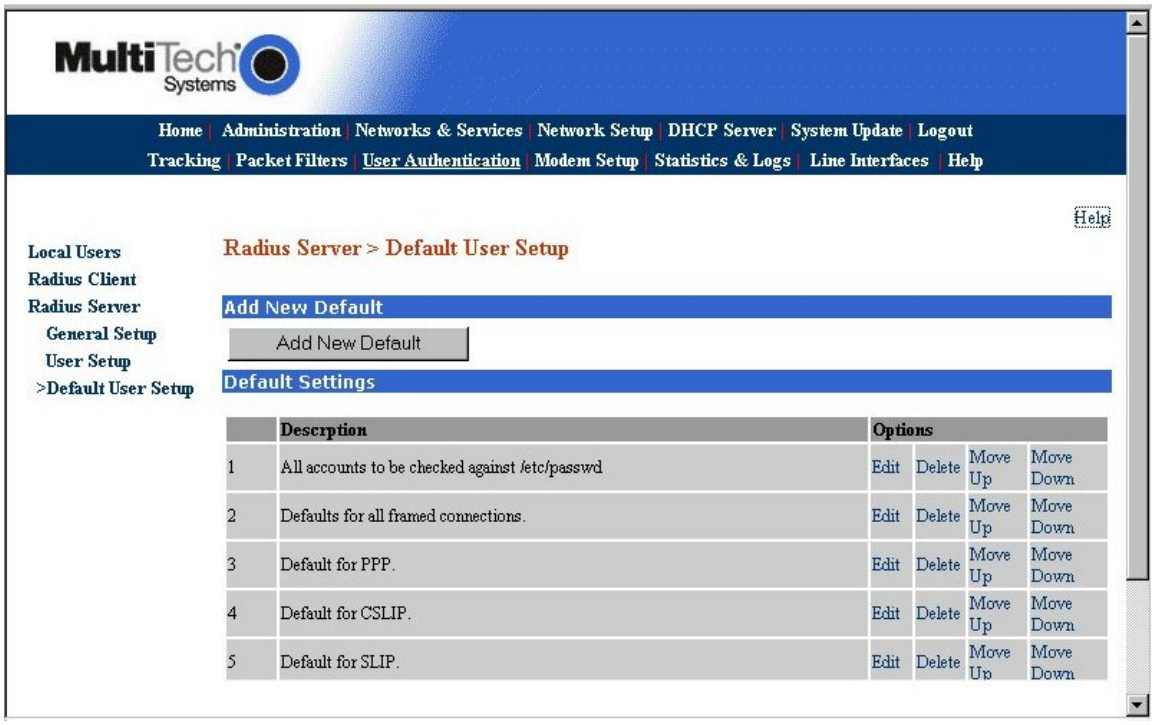
This field indicates the max allowable PPP frame size. Utimately the actual size used in a negotiated per connection.

Add

Click the Add button to this user to the Radius User data base.

User Authentication > Radius Server > Default User Setup

The Radius Server > Default User Setup screen displays the factory default settings and allows for changes to be made to the default.

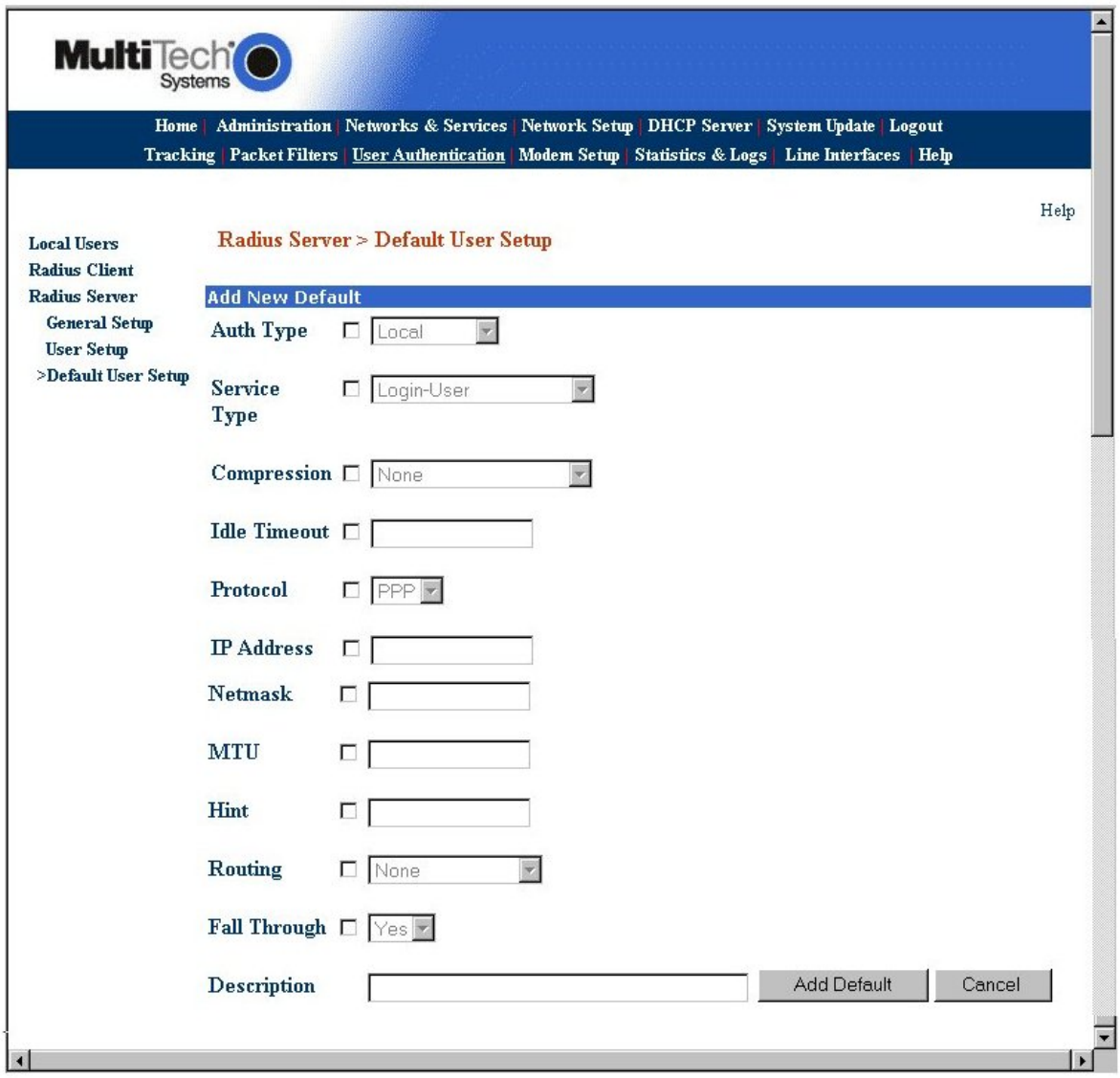

MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Local Users
Radius Client
Radius Server
General Setup
User Setup
>Default User Setup
Radius Server > Default User Setup
Add New Default
Add New Default
Default Settings
Description
Options
1 All accounts to be checked against /etc/passwd Edit Delete Move Up Move Down
2 Defaults for all framed connections. Edit Delete Move Up Move Down
3 Default for PPP. Edit Delete Move Up Move Down
4 Default for CSLIP. Edit Delete Move Up Move Down
5 Default for SLIP. Edit Delete Move Up Move Down

Default Settings

The Default Settings apply to all users of the Local Users data base. If you want to add a New Default, click on the Add New Default buttton and the Add New Default Setup screen appears.

User Authentication > Radius Server > Default User Setup

This Add New Default User Setup screen is displayed by clicking on the Add New Default button from the Radius Server > Default User Setup screen.



Auth Type

This field is for selecting the type of authentication. This field must be set to System.

Service Type

This field is for selecting the type of service the user will be requesting or provided to them.

Compression

This field is for selecting the Van Jacobson-TCP-IP compression, applies to Framed protocol PPP.

Idle Timeout

This field is for entering the maximum number of consecutive seconds of idle connection allowed before termination of the session.

Protocol
This field is for selecting the protocol to be used for framed access.

IP Address
This field indicates the IP address the framed user is to use. A value of 255.255.255.255.254 instructs the NAS equipment to give the user an IP address from an address pool defined within the NAS equipment, referred to as a dynamic IP address. A value of 255.255.255.255 instructs the NAS equipment to let the user pick it's own IP address. A unique specific value can also be defined, i.e., 206.37.212.39, referred to as a static IP address.

Netmask
This field indicates the subnet mask that should be applied to this connection.

MTU
This field is for entering the maximum allowable PPP framed size. Utilmately the actual size used in negotiation per connection.

Hint
This field is for entering additional matching criteria depending on the hint.

Routing
This field is for selecting the routing method of the user when the user is a router.

Fall Through
If this is set to Yes, it tells Radius to continue looking up other records even when the record at hand matches the request. It can be used to provide several default values or parameters.

Description
This field is for entering the description of the entry. You have to add a description in this field before you can click Add Default button. This will be displayed on the Default Settings table.

Modem Setup

The Modem Setup menu consists of three screen, Modem Usage, Modem Setup and Fax Setup. The Modem Usage screen is used to define the role of the modem. The Modem Setup screen is used to define the operating parameters of the modems set to a usage of RAS. The Fax Setup screen is used to configure various faxing parameters when at least one modem is set to the usage of Fax.

Note: The MultiAccess modems also support faxing with fax servers that are external to the MultiAccess via the Modem Sharing usage.

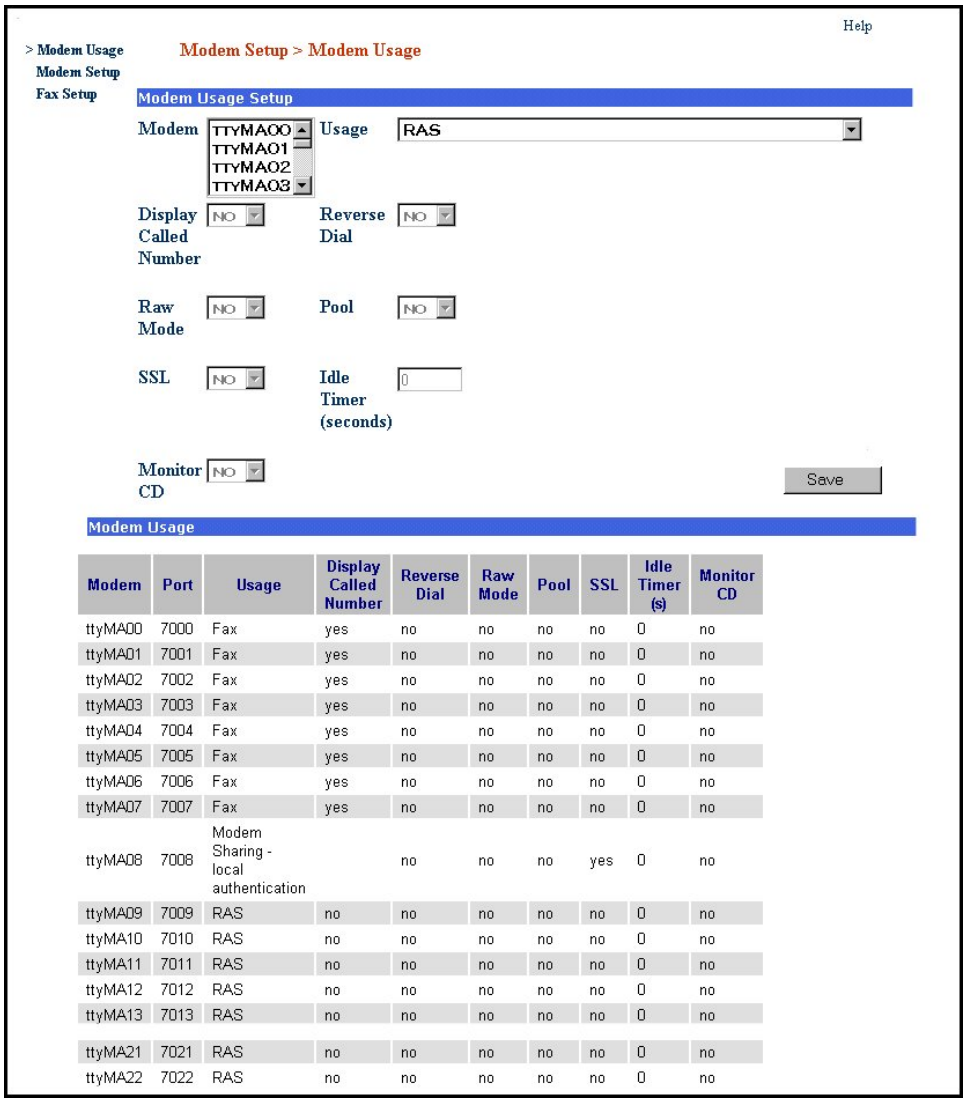
Modem Setup > Modem Usage

The modem usage screen defines whether your modems are used for standard RAS (Dial in PPP), Modem Sharing (network resource / modem pool for inbound calls with com port redirectors or proprietary inbound or outbound data), or Fax (Hylafax Server).

Defining a usage allocates the modem to a specific process within the MultiAccess operating system. Each modem is set (allocated) individually. The modem is dedicated to that usage and can not be set to more than one.

If you are using all your modems to provide dial-in PPP for your Remote Access clients, you do not have to modify the default modem usage settings, which is RAS. RAS usage is for inbound calls from PPP clients in a Dial Up networking environment.

If you are using some or all of your modems as a network resource, setting the usage to Modem Sharing, you can assign the shared modems to be part of a first available pool or each shared modem can be accessed specifically via a unique TCP port number. Each shared port can be configured to authenticate the user before giving access to the modem.



Modem	Port	Usage	Display Called Number	Reverse Dial	Raw Mode	Pool	SSL	Idle Timer (s)	Monitor CD
ttyMA00	7000	Fax	yes	no	no	no	no	0	no
ttyMA01	7001	Fax	yes	no	no	no	no	0	no
ttyMA02	7002	Fax	yes	no	no	no	no	0	no
ttyMA03	7003	Fax	yes	no	no	no	no	0	no
ttyMA04	7004	Fax	yes	no	no	no	no	0	no
ttyMA05	7005	Fax	yes	no	no	no	no	0	no
ttyMA06	7006	Fax	yes	no	no	no	no	0	no
ttyMA07	7007	Fax	yes	no	no	no	no	0	no
ttyMA08	7008	Modem Sharing - local authentication		no	no	no	yes	0	no
ttyMA09	7009	RAS	no	no	no	no	no	0	no
ttyMA10	7010	RAS	no	no	no	no	no	0	no
ttyMA11	7011	RAS	no	no	no	no	no	0	no
ttyMA12	7012	RAS	no	no	no	no	no	0	no
ttyMA13	7013	RAS	no	no	no	no	no	0	no
ttyMA21	7021	RAS	no	no	no	no	no	0	no
ttyMA22	7022	RAS	no	no	no	no	no	0	no

If you are using some or all of your modems to send or receive faxes using the integrated Hylafax server, set the modem's usage to fax. The Fax Setup menu is used to configure the integrated Hylafax server for sending and receiving faxes.

Note: Mixing usages usually requires hunt group coordination with your local telephone company, especially when mixing usages within the same Line Interface. This coordination is to avoid the collision of inbound and outbound calls or to avoid the routing of calls to a modem not set to the appropriate usage.

Modem Usage Setup

The Modem Usage Setup field contains 2 control boxes and a save button, used to change the usage of each modem. High light a modem or range of modems (tty) in the Modem scroll box. Then use the Usage pull down box to select the desired option. If the selected usage is one of the Modem Sharing options, the Displayed Called Number, Reverse Dial, Raw Mode, Pool options, Idle Timer, and Monitor CD can be enabled as needed. The SSL option can be enabled when the selected usage is one of the Modem Sharing With Authentication otpions. After selecting the desired modems and desired options, press the Save button to invoke the changes. After the screen refreshes the changes will be reflected in the Modem Usage table.

Modem

The Modem scroll box is used to select a particular modem(s) when changing it's usage.

Each modem (tty resource) is sequentially mapped to a specific channel of the digital Line Interface (for example ttyMA00 is mapped to channel 1 of Line 1, ttyMA01 is mapped to channel 2 of Line 1 and so on).

The number of available modems per Line Interface is dictated by the type of digital line. When the line interface is configured for T1-PRI, the modem usage screen displays 23 modems for example ttyM**X**00 through ttyM**X**22 (where **X** = A, B, C or D depending if the Line Interface is 1, 2, 3 or 4, respectively). When the line interface is set to T1-RBS, 24 modems are configurable (ttyMX00 thru ttyMX23). When the Line Interface is set to E1-PRI, 30 modems are configurable (ttyMX00 thru ttyMX29).

Usage

The Usage pull down menu contains 7 options. The following is a description of each Usage:

RAS - This is the default usage. New units from the factory have all ports set to RAS. When ports are added to the MultiAccess they come up set to RAS. RAS is an acronym for Remote Access Server. Ports set this way are to receive inbound calls from remote nodes (PPP clients). Mircosoft's Dial Up Networking ™ is an example of a remote node or client. The MultiAccess only supports IP (Internet Protocol) as the network protocol transported across the dial up PPP link. Refer to the User Authentication Radius Client menu to configure necessary PPP and remote host IP address parameters.

FAX - This usage allocates the modem to the intergrated Hylafax ™ Server. The Hylafax Server uses the modem to send and receive faxes. Upon receipt of an inbound fax, the Hylafax server will email the fax to the appropriate receiptiant. A Hylafax compatible Fax Client is needed to submit faxes to the server for transmitting out bound faxes.

Modem Sharing (In General) - allows the modem to be used as a network resource. The "network resource" is defined as a bank of modems residing on your IP network, available to application servers and\or individual work stations. Telnet is the TCP/IP protocol in which computers access the modems in the MultiAccess. Telnet clients (or programs that invoke telnet) must specify the appropriate TCP port number associated with the modem when opening the Telnet socket to the MultiAccess modem. Once the telnet socket is opened, the application using the modem resource has control of the modem as if it were attached locally to the machine running the application. The application can make the modem dialout or answer incomng calls and control it's behavior (speed, modulation & error control protocols, etc) via the use of AT commands.

A common dial out modem sharing application is where Com Port Redirector software (such as Multi-Tech's WINMCSI) is installed on network workstations that have IP access to the MultiAccess. The redirector software adds a virtual com port to the workstation. When an application uses this virtual com port, it's data is redirected to and from the MultiAccess modem.

A common dial in modem sharing application is where a proprietary host application, running on a sever that has IP access to MultiAccess, opens multiple telnet sockets (one to each modem) to the MultiAccess. When the sockets are opened, the application can look for incoming calls\rings, instruct the modem to answer and then process data from the remote end. The application can also originate calls to remote locations if it so chooses by instructing the modem to dial.

Modem Sharing - no authentication - When a Telnet client opens a socket to the MultiAccess, access is immediately given to the modem. Take care to secure access to these ports via firewall or IP filter rules to prevent unwanted access.

Modem Sharing - local authentication - When a Telnet client opens a socket to the MultiAccess, a login prompt is issued by the Multiaccess to the client trying to use the resource. The client/user must supply a valid set of credentials (defined in the Local User data base), before access is granted. The Local User database is found in the User Authentication menu.

Modem Sharing - radius authentication - When a Telnet client opens a socket to the MultiAccess, a login prompt is issued by the Multiaccess to the client trying to use the resource. The client/user must supply a valid set of credentials (defined in the RADIUS User data base), before access is granted. The RADIUS User database is a variable depending if your RADIUS server is external to the MultiAccess or if you are using the internal RADIUS server. See the User Authentication group of menus for more details.

Modem Sharing - local & radius authentication - When a Telnet client opens a socket to the MultiAccess, a login prompt is issued by the Multiaccess to the client trying to use the resource. The client/user must supply a valid set of credentials defined in either the Local User database or the RADIUS User database, before access is granted. All credentials are normally checked against the RADIUS data base. If the RADIUS server rejects the credentials, access to the modem resource is denied. If the user is to authenticate against the Local database they must include an ! (exclaimation point) in front of the username. The ! is a flag used to instruct the authenticator process to check the Local User database instead of the RADIUS database. For example if the administrator of the Multiaccess adds a username of “Bob” with a password of “J3imK!123” to the Local User database, when the user provides the credentials the username would be entered as “!Bob” with no change to the password.

Custom - Custom usage is reserved for when a 3rd party application is installed into the Linux OS, in which the MultiAccess RAS, Fax, or Modem Sharing programs do not attempt to control or use the tty modem ports.

Modem Usage Setup - Modem Sharing

The following parameters only apply after the usage is Modem Sharing.

Display Called Number

This parameter applies to inbound (received) calls when the Line Interface type is PRI. The telephone number (or final digits) dialed by the originator will be displayed into the telnet socket following the first “ring” message. The Called Number information (string of digits) is provided by the central office switch and is commonly referred to as DNIS. The MultiAccess does not support DNIS when the Line Interface type is T1-RBS.

Reverse Dial

This parameter enables two features, comma dialing and reverse dial mode. When enabled, the dial string can include the use of commas, used to create a pause between digits of the dial string (most commonly used to specify the extension of the answering modem).

Example: “atdt18003334444,,,,,4321”. Each comma creates a 2 second pause. 4321 is the extension of the desitination phone line\modem.

Reverse dial mode is where the dial string includes the letter “r” at the very end of the dial string, the purpose of which is to instruct the MultiAccess modem to switch from originate to answer mode after dialing. For example: “atdt17637175549r”.

Please Note: When Reverse Dial is enabled, the dial string must include the tone (t) command, for example, atd**t***string* .

Raw Mode

"Yes" sets the Telnet TCP port to a RAW socket. User data is treated "as is" (without interpretation) and Telnet Command Escape capability is disabled.

"No" allows the Telnet command parser to look for escape sequences that are used to communicate control fucntions. A common example is to support RFC-2217 Com Port Control.

Pool

Selecting yes or no determines the TCP port number that is assigned to the modem. When yes is selected the TCP Port number assigned to the selected modem(s) is set to 6000. When a computer on the LAN opens a Telnet connection specifiying port 6000, the MultiAccess routes the session to the first available modem starting with the lowest tty that is set to 6000. If you want to access a specifc modem, accept the default of No. Each selected modem will be given a specific TCP port number, starting at 7000 +.

Note: A modem/tty port can **not** be set to both 6000 and 7000+ port numbers.

SSL – Secure Sockets Layer

This Pull down only applies when the usage is Modem Sharing with Authentication. SSL is a transport level technology for authentication and data encryption. SSL negotiates a secure point-to-point socket using pre determined Site Certificate information. Site Certificate information is used to authenticate the user and encrypt the data. Site Certificate information is configured in the Administration menu. This option should only be used with SSL capable Telnet clients.

Idle Timer

The Idle Timer, upon expiring, will hangup the modem and close the telnet socket. Idle time is defined as no data flow in both directions. Any data sent or received across the socket will cause the Idle Timer to start over. When there has been no data activity for the duration specified, the idle timer will expire.

Monitor CD

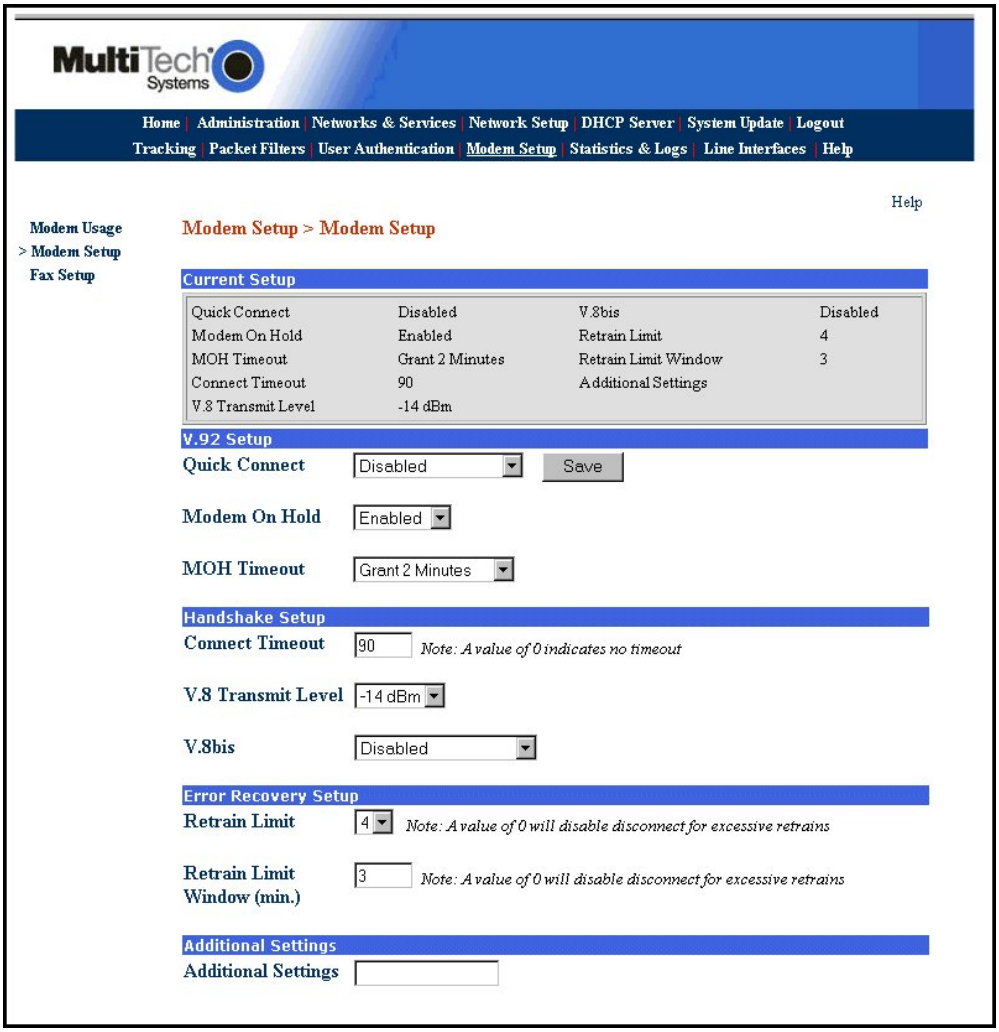
Upon the modem disconnecting, the MultiAccess will close the telnet socket.

Modem Usage

The Modem Usage table displays each modem (tty name), it's (TCP) Port number, Usage, if the TCP port is RAW, if it's in a first available pool or not, whether SSL is enabled, and other options of Idle Times and Monitor CD. When the modem Usage is RAS, FAX, or Custom, only Modem and Usage columns apply.

Modem Setup > Modem Setup

This screen applies to all the modems set to a RAS usage. This screen allows you to set the parameters most important for modem performance. Parameters such as the time to establish a connection, whether to enable the modem-on-hold feature, error recovery, etc.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Modem Usage
> Modem Setup
Fax Setup
Modem Setup > Modem Setup
Current Setup
Quick Connect Disabled
Modem On Hold Enabled
MOH Timeout Grant 2 Minutes
Connect Timeout 90
V.8 Transmit Level -14 dBm
V.8bis Disabled
Retrain Limit 4
Retrain Limit Window 3
Additional Settings
V.92 Setup
Quick Connect Disabled Save
Modem On Hold Enabled
MOH Timeout Grant 2 Minutes
Handshake Setup
Connect Timeout 90 Note: A value of 0 indicates no timeout
V.8 Transmit Level -14 dBm
V.8bis Disabled
Error Recovery Setup
Retrain Limit 4 Note: A value of 0 will disable disconnect for excessive retrains
Retrain Limit Window (min.) 3 Note: A value of 0 will disable disconnect for excessive retrains
Additional Settings
Additional Settings

V.92 Setup

Quick Connect – You can enable or disable Quick Connect or select Short Phase 1 only or Short Phase 2 only. V92 Quick Connect is a feature that allows V92 clients to use previously obtained line quality configuration data to speed up portions of the negotiation process.

Disabling this feature dictates the modems should use configuration data determined by a line probe during the negotiation process. Enabling this feature allows the V92 client to dictate configuration information used for both the V8 portion (phase 1) and the modulation portion (phase 2).

Note: Line conditions can change. With this feature enabled and if line conditions change, it could actually increase the connect time slightly.

Modem On Hold – You can enable or disable the Modem-On-Hold feature from the drop down box. Modem On Hold (MOH) requires the remote MOH capable V92 client to use a line that has a subscriber service of “Call Waiting” or “Caller ID Call Waiting”. MOH allows the client system to put the RAS call (Internet Connection) on hold so it can answer the call waiting.

MOH Timeout – You can select the timeout period for the Modem-On-Hold feature. The selections are Deny MOH, Grant 10 Seconds to Grant 16 minutes. This is the time the modem connection is put on hold. This value is relayed to the remote client when the hold request is initiated.

Handshake Setup

Connect Timeout – This sets the time, in seconds, within which Modem Carrier must be established. If the modem has not connected when this time has elapsed, the attempt is aborted.

V.8 Transmit Level – This provides a list of available levels. The available choices are from -9 dBm to -20 dBm. -20 dBm is less power than -9 dBm.

V.8bis – You can select Disable, or Enable Without V.90 or Enabled with V.90. V.8bis is used to negotiate K56flex™ connections.

Note: Selecting “V8bis Enabled **Without** V90” does NOT disable V.90, it changes where it is offered.

Error Recovery Setup

Retain Limit – This value along with the Retrain Limit Window value is used to define excessive retrains. Excessive retrains will cause the modem to disconnect. The Retrain Limit value defines the max number of retrains allowed within the Limit Window. When this is set to zero, the port will not disconnect due to excessive retrains.

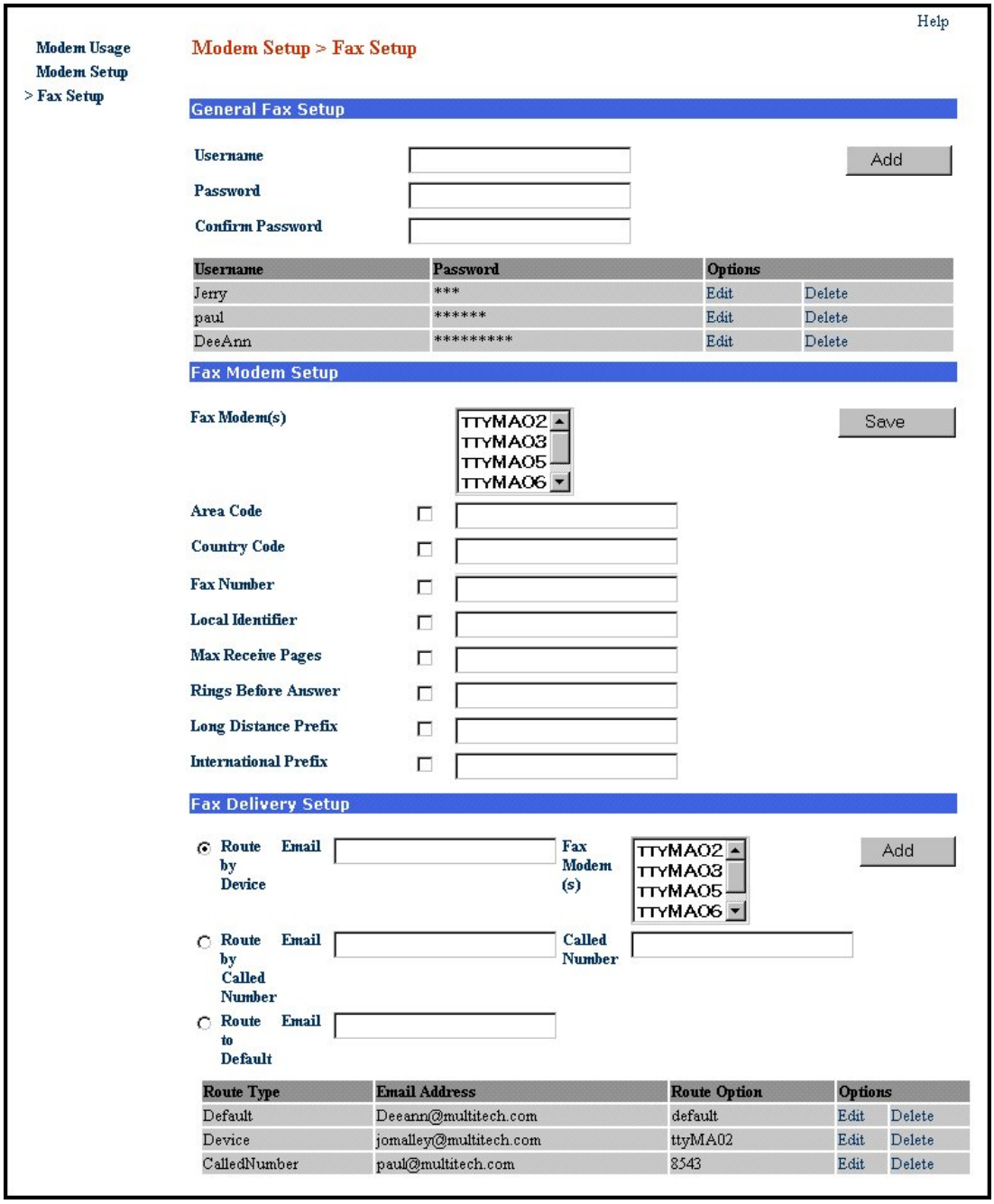
Retain Limit Window – This specifies the window duration, in minutes, within which to check for excessive retrains. When this is set to zero, the port will not disconnect due to excessive retrains.

Additional Settings

Additional Settings – This allows you to add additional commands to the initialization string. This should contain only additional commands and not the AT itself. Appendix B provides a detailed description of the AT commands supported by the MultiAccess.

Modem Setup > Fax Setup

The Fax Setup screen is used to configure the internal Hylafax server. If no modems are set for fax usage, only the General Fax Setup section is displayed. A Hylafax compatible fax client, like the Multi-Tech FaxFinder Client (a copy of which is found on the software CD that ships with the MultiAccess) is needed to send faxes via the MultiAccess to remote dial-up fax destinations. The General Fax Setup field establishes a data base of credentials used by fax clients to log into the Hylafax server (preventing unauthorized use of the Hylafax server). Inbound faxes (received by Hylafax from remote dial-up fax locations) are sent as .tif attachments to emails generated by the Hylafax server. The Fax Modem Setup group sets the port identification and other administrative details. The Fax Delivery Setup group defines how incoming faxes are distributed.



Inbound faxes are sent as .tif attachments to emails generated by the MultiAccess. Hylafax converts the contents of the fax (all pages) into one .tif file and attaches it to the email. The full name of the attachment will

be “fax##########.tif” were ###…is equal to the numeric value of the total number of faxes received by the Hylafax server. The sender of the email (“From” header) will be identified as “The HylaFax Receive Agent”. The subject of the email will identify who sent the facsimile, “Facsimile Received From CSID”, if the CSID is provided by the remote fax location. The body of the email will include the following details about the attached fax; sender’s CSID, number of pages, resolution quality, time and date it was receieved, time to receive, signal rate, data/compression format, ECM mode and the local identifier.

General Fax Setup

Username & Password

The Username and Password windows are used to create a database of fax client credentials. Install the fax client on each workstaion you wish to send faxes from. The fax client must use credentials defined here to log into the Hylafax™ server before submitting faxes for sending. All Fax Clients can use the same set of credentials, or you may add a set of credentials per client. The fax client uses FTP on TCP port 4559 to submit faxes to the Hylafax™ server. The Fax Client is not used for receiving faxes.

Fax Modem Setup

The Fax Modem Setup fields are used to configure the fax station identity and other administrative variables. The default settings are normally sufficient with the exception of the “Rings Before Answer” parameter. When the Called Number feature is used, the Rings Before Answer must be set to 2 for all the ports. Each Fax Modem is to be configured with a unique Local Identifier, which is used as the TSI (Transmit Station Identifier) when sending faxes and is included in the body of the email when receiving faxes. You can limit the maximum number of pages being received.

Fax Modem

The Fax Modem scroll box allows you to high light a range of modem ports for assigning global parameters or high lighting individual ports for port specific parameters.

Local Identifier

The Local Identifier is included in the message body of the email. The default identifier is the tty port name.

Max Receive Pages

The default value is 25 pages. Limiting the number of pages is discretionary.

Rings Before Answer

Rings Before Answer option is for incoming faxes. The default value is 1. If the Route By Called Number option is enabled, the Rings Before Answer must be set to 2.

Fax Delivery Setup

The Fax Delivery Setup section defines how incoming faxes are routed to recipient; by device, by called number, or route to default, if undetermined. The Fax Delivery options are established by activating an option, entering an email address, defining a port for the Route by Device option, or entering a Called Number which is defined by your service provider.

Route by Device

This fax delivery setup allows all incoming faxes on a particular port to be delivered to a specific email address. When this option is selected, an email address is entered in the Email window and the port is defined by highlighting a Fax Modem. When the Add button is clicked, the MultiAccess updates the software and then the entry is shown in the listing at the bottom of the screen. For example, click on Route by Device option, enter jomalley@multitech.com in the Email window, and for this example I highlighted ttyMA02 as the modem port. So now, any fax that comes on ttyMA02 is going to be sent to Jomalley@multitech.com.

Route by Called Number

Route by Called Number is a dynamic delivery method that requires the use of a PRI line (T1-PRI or E1-PRI line type). The "Called Number" refers to the DNIS information provided per call by Telco. The objective is to associate the DNIS information to an email address. The Route by Called Number feature requires the modem(s) to answer on two rings.

The Telco switch will (via PRI signaling) provide DNIS digits to the MultiAccess at the time of ringing (call setup). The Hylafax Server will see the 1st "ring" progress message come from the modem, then the DNIS information will be displayed, followed by the 2nd "ring" message. After the second ring, Hylafax will instruct the modem to answer and receive the incoming fax. When the Fax is complete, Hylafax will reference the Fax routing table and match the DNIS information to an email address. If no Called Number route entries can be matched to the DNIS information for that particular fax - the Route to Default entry will be used.

How many DNIS digits will Telco be providing? The remote originator of the fax may dial 11 digits (1-800-333-4444) but Telco may only provide the last x number of digits dialed (where x is commonly = 4) as the DNIS information. The DNIS digits provided by Telco is a variable to be determined at the time of ordering and installing the PRI service.

Route to Default

Route to Default fax rule is used when the other routing rules are not defined or can not be matched. To establish the Route to Default option, click on Route to Default and then enter the email address of the recipient, for example Administrator@multitech.com, in the corresponding Email window.

Statistics & Logs

The Statistics & Logs group of menus is used to view current status and obtain historical information of the MultiAccess system. The Statistics & Logs menu contains the follow sub menus:

- Setup - Defines the refresh rate for certain menus.
- Uptime - Displays the duration of continuous operation and the date and time since the server last booted.
- Networks - Displays; Interface Details, Routing Table, and Network Connections.
- Line Interface Status - Displays the current layer 1 status of each digital line interface (alarm condition).
- Modem Connections - Displays the current state of all modems, along with connection protocol details, Caller ID information and Call History information.
- Server Connections - Displays who is currently logged into the unit and via what means.
- Interfaces - Graphically displays the Ethernet utilization for each interface by days, weeks, months and Yearly.
- Accounting - When enabled, displays daily byte totals transmitted and received for the interface.
- Self Monitor - Displays basic status of specific internal processes (daemons).
- View Logs - allows for system log files to be displayed on screen or saved to disk.

Administrators should become familiar with patterns and messages, so that it can be recognized when something changes or goes wrong.

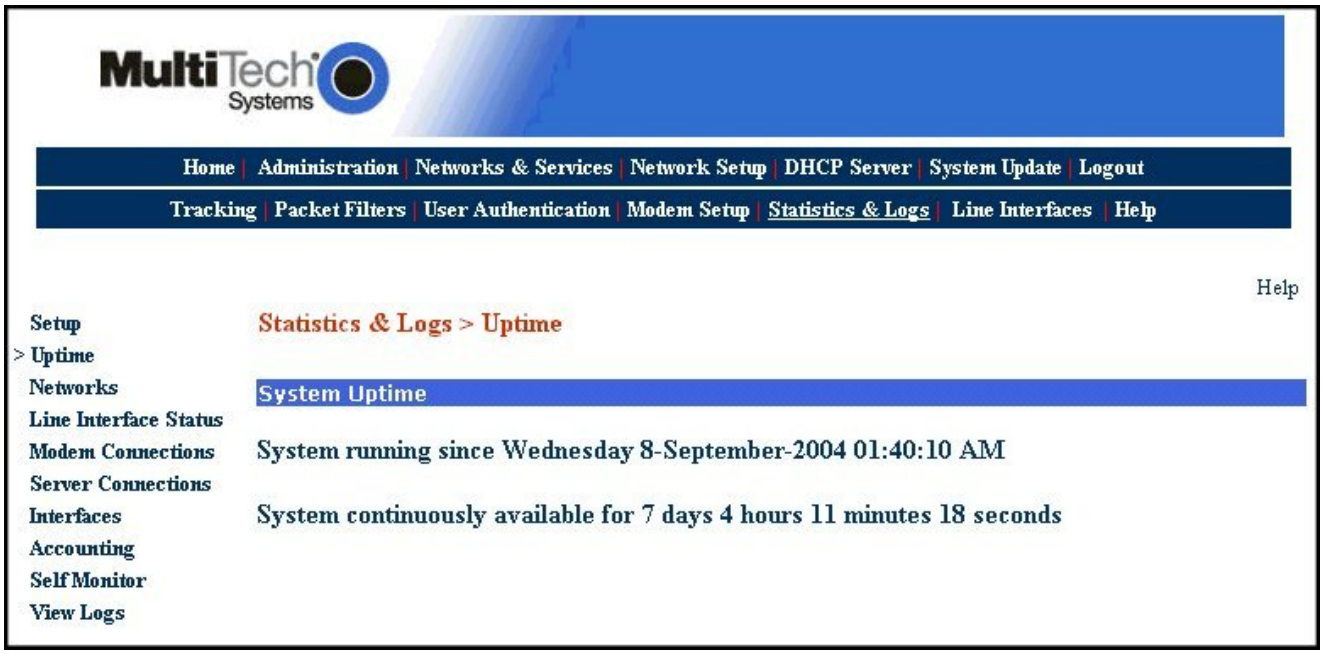
Statistics & Logs > Setup

Certain screens within the Statistics & Log menu group will automatically refresh. An automatic screen refresh is equivalent to clicking on the refresh icon in your browser's tool bar (or pressing the F5 key). The value selected applies to all of the menus that automatically refresh (Line Interface Status, Modem Connections, Modem Connection Details, Modem Connection Caller ID, and Server Connections). The minimum refresh rate is once every 15 minutes and the maximum is once every 30 seconds.

Note: Web caching rules applied by computers and programs external to the MultiAccess may prevent or effect the refreshing of page content.

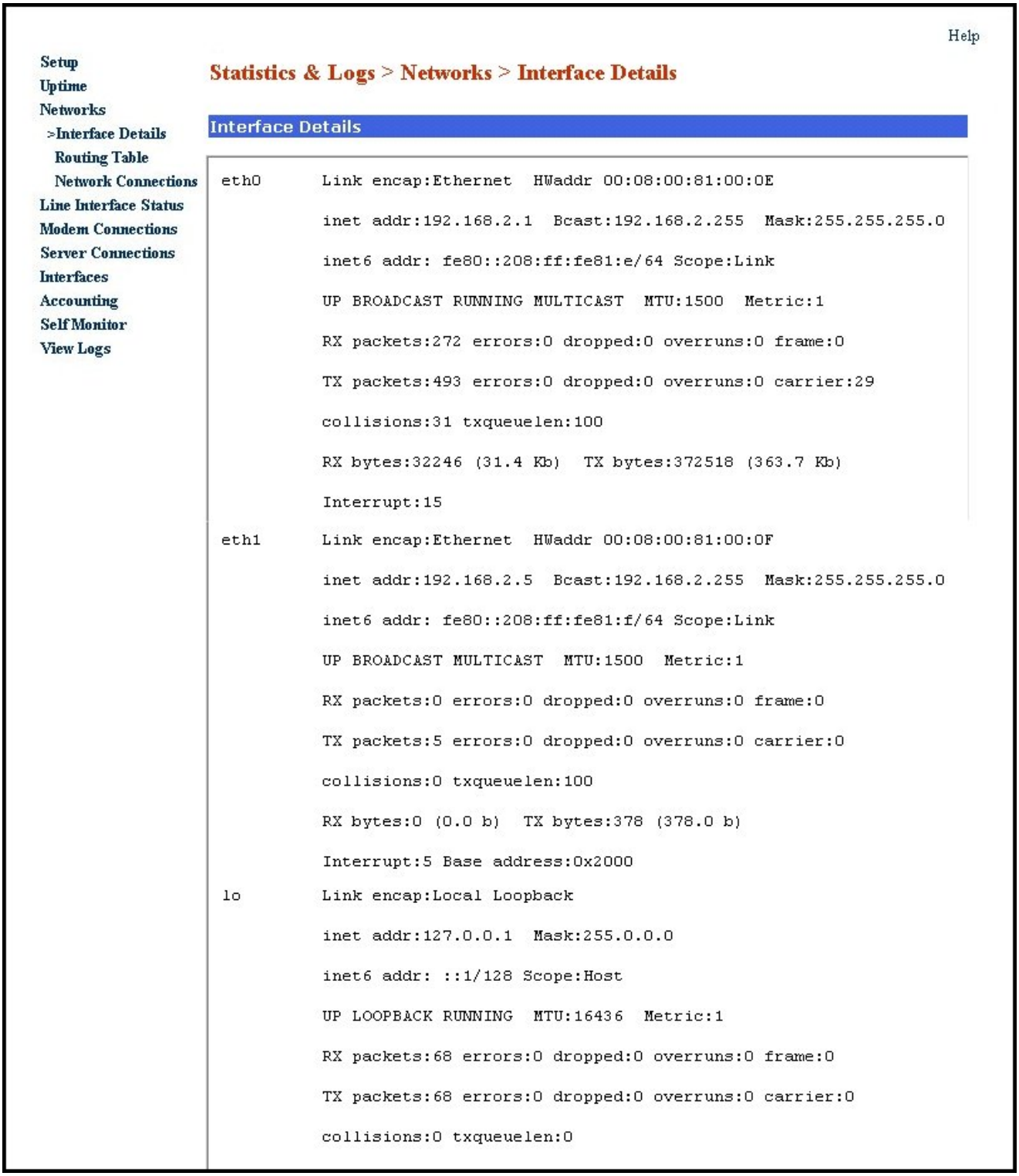
Statistics & Logs > Uptime

Uptime tells you how long the system has been running. The first line displays the date and time the system was started. The second line displays the total time elapsed since the system was started in days, hours, minutes, and seconds.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Setup
> Uptime
Networks
Line Interface Status
Modem Connections
Server Connections
Interfaces
Accounting
Self Monitor
View Logs
Statistics & Logs > Uptime
System Uptime
System running since Wednesday 8-September-2004 01:40:10 AM
System continuously available for 7 days 4 hours 11 minutes 18 seconds

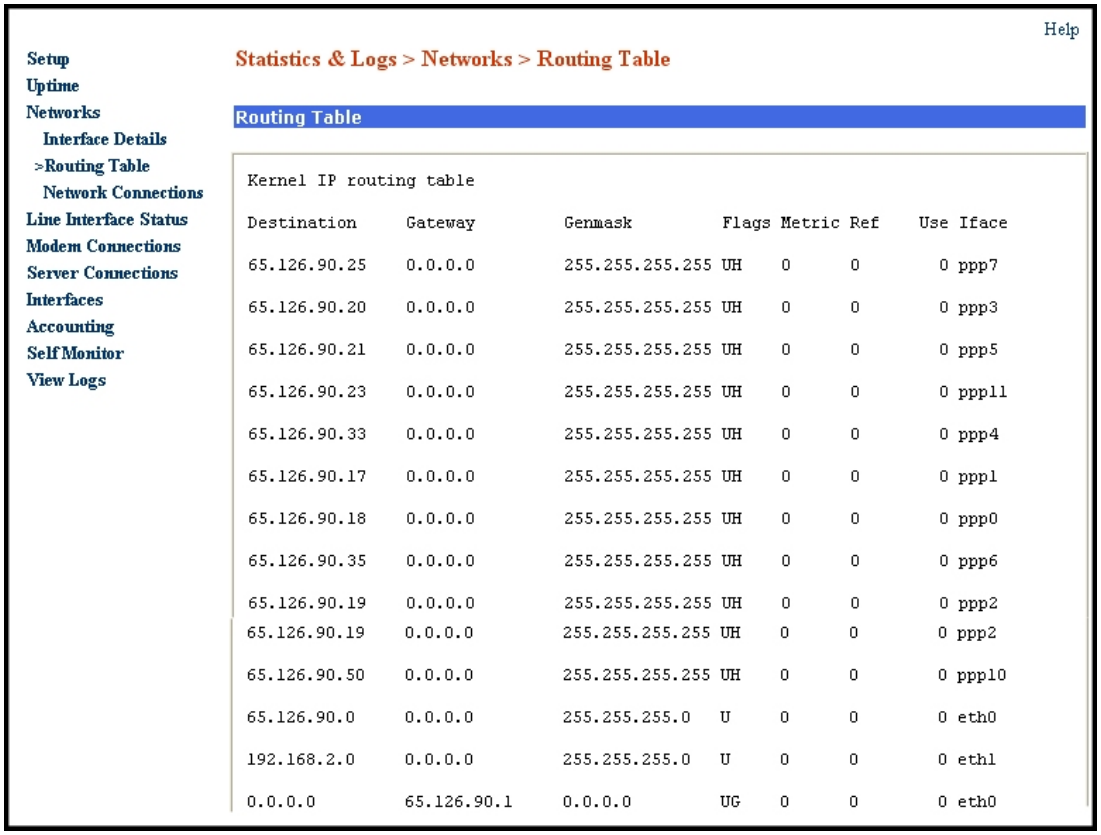
Statistics & Logs > Networks

The Interface Details screen will summarize configuration and performance information for each network interface. Both Ethernet interfaces and the internal Loopback interface will always be present in this screen. PPP interfaces will be added and removed automatically to and from the table, as the PPP connections are established and relinquished.



Routing Table

This screen displays the current kernel routing table. The table will always reflect the two permanent ethernet interface routes. Routes pertaining to PPP connections are automatically added and removed as the connections are established and relinquished. This table will also reflect static and interface routes added manually via the Network Setup>Routes menu.



The routing table is organized in the following columns:

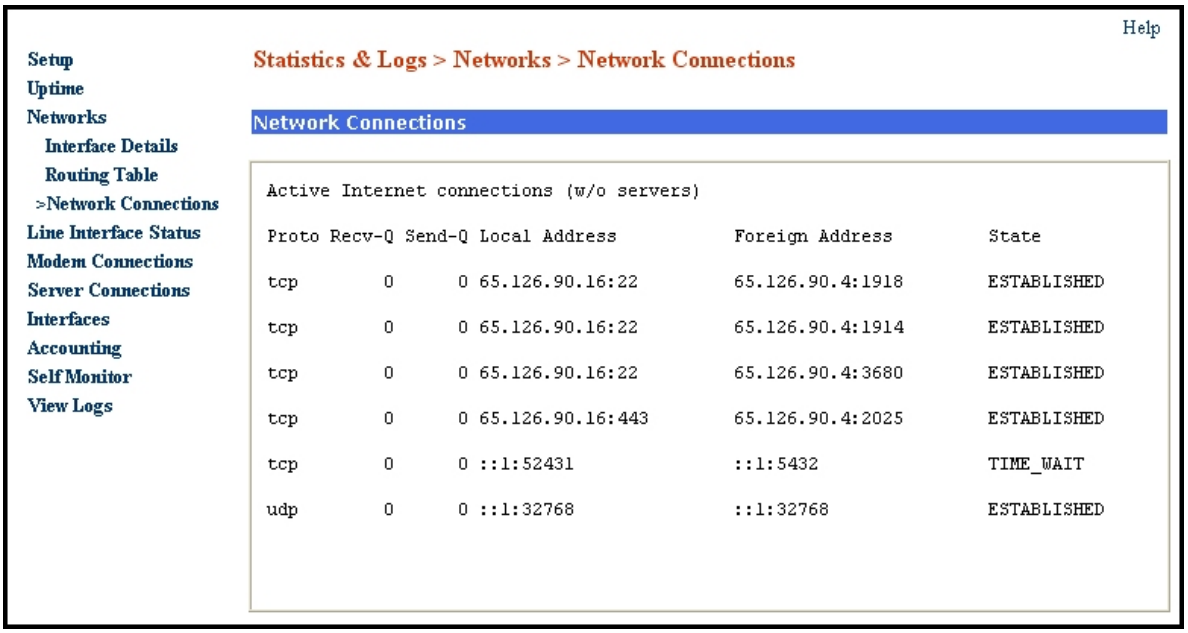
Destination - The destination network or destination host.
Gateway - The gateway address or '*' if none set.
Genmask - The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route.
Flags - Possible flags include:

- **U** - route is up
- **H** - target is a host
- **G** - use gateway
- **R** - reinstate route for dynamic routing
- **D** - dynamically installed by daemon or redirect
- **M** - modified from routing daemon or redirect
- **A** - installed by addrconf
- **C** - cache entry
- **!** - reject route

Metric – The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Ref - Number of references to this route (not used in the MultiAccess).
Use - Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).
Iface - Interface to which packets for this route will be sent.

Network Connections

Click the **Network Connections** to display the status of all current (active) network connections to or from your system. Information on the active protocol, receive queue, send queue, local address, foreign address, and current state is shown for each of the MultiAccess's active Internet connections. It also shows you all of the established TCP sessions and all of the TCP and UDP ports that the MultiAccess is listening to for incoming connections. Connections through the MultiAccess are not shown.



Proto - Protocol tcp, udp, and raw are used by the socket.

Recv-Q- Receive Queue – The count of bytes not copied by the user program connected to this socket.

Send-Q- Send Queue – The count of bytes not acknowledged by the remote host.

Local Address- IP address and port number of the local end of the socket.

Foreign Address- IP address and port number of the remote end of the socket. If the final remote end point is actually on a different network, the foreign address will be that of the first hop, interface of the router off the local network.

State - The state of the socket. Normally this can be one of several values:

ESTABLISHED - The socket has an established connection.

SYNC_SENT - The socket is actively attempting to establish a connection.

SYN_RECV- A connection request has been received from the network.

FIN_WAIT1- The socket is closed, and the connection is shutting down.

FIN_WAIT2- Connection is closed, and the socket is waiting for a shutdown from the remote end.

TIME_WAIT- The socket is waiting after close to handle packets still in the network.

CLOSED- The socket is not being used.

CLOSE_WAIT- The remote end has shut down, waiting for the socket to close.

LAST_ACK- The remote end has shut down, and the socket is closed. Waiting for acknowledgement.

LISTEN- The socket is listening for incoming connections.

CLOSING – Both sockets are shut down but we still don't have all our data sent.

UNKNOWN – The state of the socket is unknown.

How to Read the Network Connections Table - Example 1

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	65.126.90.16:22	65.126.90.4:1918	ESTABLISHED

This output tells you there is an active (**ESTABLISHED**) connection from **65.126.90.16** port 22 (http) to **65.126.90.4** port 1918.

How to Read the Network Connections Table - Example 2

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN

This output tells you that your MultiAccess is listening (**LISTEN**) at all (**0.0.0.0**) interfaces for incoming requests to port 22 (ssh); the remote IP address is **ANY** (**0.0.0.0**) and the remote port does not care (the ***** in the **Foreign Address** column indicates **ANY**).

Statistics & Logs > Line Interface Status

This screen displays a snap shot of the layer one status of each digital line interface that is enabled. The digital line interfaces will automatically be enabled upon installation of an MA30EXP modem module (into the corresponding slot on the motherboard). The information displayed reflects the status of the interface's receiver circuitry.

MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Setup
Uptime
Networks
> Line Interface Status
Modem Connections
Server Connections
Interfaces
Accounting
Self Monitor
View Logs
Statistics & Logs > Line Interface Status
Line Interface Status
Line 1 : No Alarms - Active
D Channel Status: Active
Framer Status: 64 0 0 0 0
Framing Error: 0 0
Code Violation: 0 0
CRC Error: 0 0
Errored Block: 0 0
Bit Error: 0 0
DL-Bit: 231 119 126
Line 2 : No Alarms - Active
D Channel Status: NA
Framer Status: 64 0 0 0 0
Framing Error: 0 0
Code Violation: 0 0
CRC Error: 0 0
Errored Block: 0 0
Bit Error: 0 0
DL-Bit: 0 0 0
Line 3 : No Module Installed
Line 4 : No Module Installed

The overall status of the interface is listed first, stating the alarm status and activity status. The D Channel Status applies when the line interface is configured for T1PRI or E1PRI and connected to a T1or E1 PRI ISDN line (T1RBS lines do not have a D Channel). The 3rd item listed is the Framer Status, this numerical value is read by the system to determine the layer one status. Various bit error registers are also listed. The final category listed is the DL-Bit, which displays the contents of the Facility Data Link channel of an Extended Super Frame.

No Alarm Active - means the line interface is receiving a properly framed signal and that at least one modem associated with this line interface has a call in progress. The front panel LEDs will reflect the LA on solid, with the LC and LS off.

No Alarm Inactive - means the line interface is receiving a properly framed signal and that all modems associated with this line are waiting to establish a call. The front panel LEDs will reflect the LA on solid, with the LC and LS off (same as above).

Red Alarm - is equal to Los of Signal. This will be displayed when the line cable is unplugged (or similar termination or wiring problem), or when the signal present on the line is smaller than the expected level defined by the "Receive Sensitivity" setting. The front panel LEDs will reflect the LC on solid, with the LA and LS off.

Yellow Alarm - is a specific layer 1 pattern detected within a properly framed signal. A yellow alarm indicates the remote end is experiencing a problem (of a various nature). Yellow alarm is also known as RAI (Remote Alarm Indication). When the MultiAccess indicates (receives) a yellow alarm, it means it's receiver circuitry is

working properly and that the problem is at T1/E1 equipment down the line from (remote to) the MultiAccess. The front panel LEDs will reflect the LS on solid, with the LA and LC off.

Loss of Frame Alignment - is reported by the line interface when it is unable to synchronize with the incoming signal. This is most likely due to a timing problem on the line or a mismatch in framing format settings. The front panel LEDs will reflect the LA flashing, with the LC and LS off.

Blue Alarm - is equal to AIS (Alarm Indication Signal). Like the yellow alarm, it is a signal the MultiAccess receives from the line and indicates the problem is remote to the MultiAccess. The AIS pattern is a constant stream of unframed ones. AIS is usually an indication of an end to end physical or logical failure and that it is most likely on the other side of the immediate Telco equipment we are communicating with. The front panel LEDs will reflect the LA flashing, with the LC and LS off.

Regarding the various bit error counters, these counters will not increment on a clean T1\E1 line. If these types of errors do occur, these fields are not updated on this screen. Instead, any change to these counters will be entered into the kernel log file (messages file) as FALC events (as the changes occur). Bit errors can cause individual modem problems (no connects, sluggish performance and disconnects). Please Note, a change in Layer 1 status are also written to the log file as they occur.

The following are some example messages.

The log file will contain the following sequence of messages when a red alarm condition occurs.

Jul 28 14:30:31 multiaccess kernel: FALC 800:
Jul 28 14:30:31 multiaccess kernel: fech = 0, fecl = 4
Jul 28 14:30:31 multiaccess kernel: cvch = 0, cvcl = 0
Jul 28 14:30:31 multiaccess kernel: cech = 0, cecl = 0
Jul 28 14:30:31 multiaccess kernel: ebch = 0, ebcl = 0
Jul 28 14:30:31 multiaccess kernel: bech = 0, becl = 0
Jul 28 14:30:31 multiaccess kernel: Red Alarm on falc 800

The following sequence is an example of logged messages when the line recovers from a red alarm condition.

Jul 28 14:32:31 multiaccess kernel: Red Alarm Recovered on falc 800
Jul 28 14:32:31 multiaccess kernel: Loss Frame Alignment but not LOS on falc 800
Jul 28 14:32:31 multiaccess kernel: Link is active on falc 800

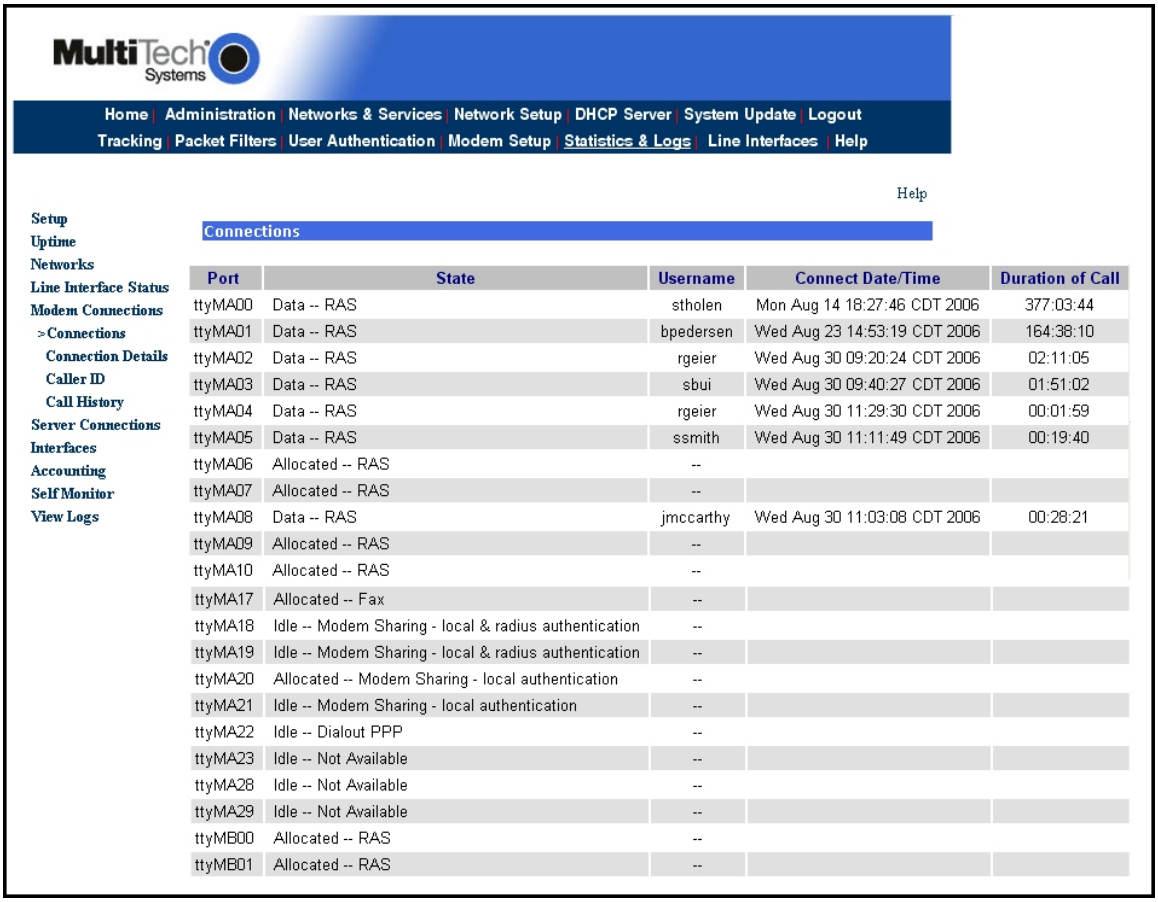
The following example displays a burst of line code bi-polar violation errors.

Jul 28 14:35:17 multiaccess kernel: FALC 800:
Jul 28 14:35:17 multiaccess kernel: fech = 0, fecl = 0
Jul 28 14:35:17 multiaccess kernel: cvch = 0, cvcl = 3
Jul 28 14:35:17 multiaccess kernel: cech = 0, cecl = 0
Jul 28 14:35:17 multiaccess kernel: ebch = 0, ebcl = 0
Jul 28 14:35:17 multiaccess kernel: bech = 0, becl = 0
Jul 28 14:35:18 multiaccess kernel: FALC 800:
Jul 28 14:35:18 multiaccess kernel: fech = 0, fecl = 0
Jul 28 14:35:18 multiaccess kernel: cvch = 0, cvcl = 2
Jul 28 14:35:18 multiaccess kernel: cech = 0, cecl = 0
Jul 28 14:35:18 multiaccess kernel: ebch = 0, ebcl = 0
Jul 28 14:35:18 multiaccess kernel: bech = 0, becl = 0

The letters ch is count high and cl is count low, fe is frame errors, cv is bi-polar violations, ce is crc errors, eb is errored blocks and be is bursty errors.

Statistics & Logs > Modem Connections

The Modem Connections group of menus contains Connections, Connection Details, Caller Id and Call History screens. The Connections, Connection Details and Caller ID screens provide various details about the current state of each modem in the system. The Call History screen maintains a record of all calls that establish carrier.



Port	State	Username	Connect Date/Time	Duration of Call
ttyMA00	Data -- RAS	stholen	Mon Aug 14 18:27:46 CDT 2006	377:03:44
ttyMA01	Data -- RAS	bpedersen	Wed Aug 23 14:53:19 CDT 2006	164:38:10
ttyMA02	Data -- RAS	rgeier	Wed Aug 30 09:20:24 CDT 2006	02:11:05
ttyMA03	Data -- RAS	sbui	Wed Aug 30 09:40:27 CDT 2006	01:51:02
ttyMA04	Data -- RAS	rgeier	Wed Aug 30 11:29:30 CDT 2006	00:01:59
ttyMA05	Data -- RAS	ssmith	Wed Aug 30 11:11:49 CDT 2006	00:19:40
ttyMA06	Allocated -- RAS	--		
ttyMA07	Allocated -- RAS	--		
ttyMA08	Data -- RAS	jmccarthy	Wed Aug 30 11:03:08 CDT 2006	00:28:21
ttyMA09	Allocated -- RAS	--		
ttyMA10	Allocated -- RAS	--		
ttyMA17	Allocated -- Fax	--		
ttyMA18	Idle -- Modem Sharing - local & radius authentication	--		
ttyMA19	Idle -- Modem Sharing - local & radius authentication	--		
ttyMA20	Allocated -- Modem Sharing - local authentication	--		
ttyMA21	Idle -- Modem Sharing - local authentication	--		
ttyMA22	Idle -- Dialout PPP	--		
ttyMA23	Idle -- Not Available	--		
ttyMA28	Idle -- Not Available	--		
ttyMA29	Idle -- Not Available	--		
ttyMB00	Allocated -- RAS	--		
ttyMB01	Allocated -- RAS	--		

The Connections screen displays the state of each port, how it's allocated, who is using it and the start time and duration of the current call.

The Port is a combination of serial tty and modem resource. The State column reflects three aspects; the port's availability as a resource to the Linux system, the status of the modem and the modem's usage configuration. The usage directly effects the state of the port. The state of "idle" means the port, as a system resource, is available to the system and currently is not in use.

The state of "allocated" means as a system resource, it is being used. When the modem's usage is set to RAS or FAX, the state of the port is "Allocated". When a successful call is established, the state will change from Allocated to Data. When the call is finished, the state will return to Allocated.

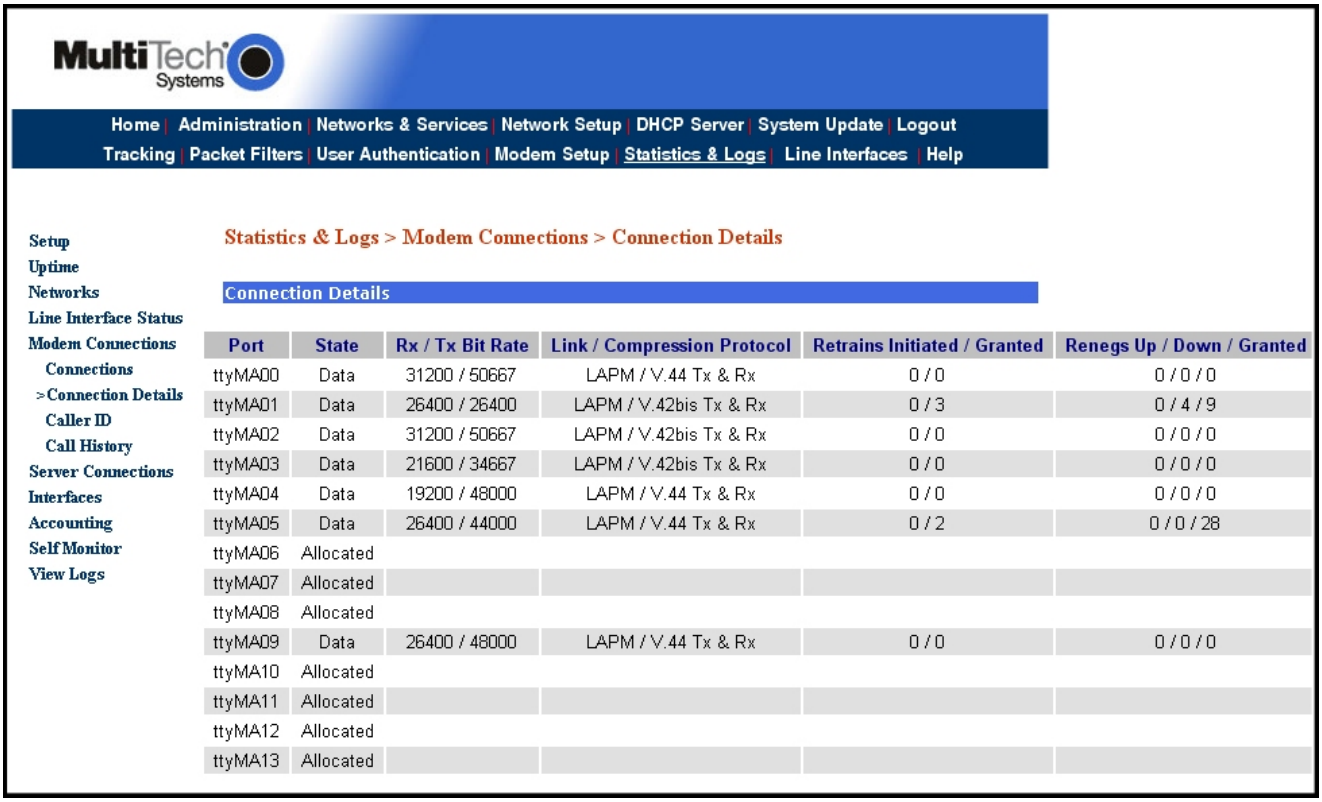
When the modem's usage is set to one of the Modem Sharing options, the state of the port is "Idle". When the TCP socket to the modem is successfully opened by a network based application, the state will change to Allocated. When the network based application makes the modem dial or answer and if successful, the state will change to Data. When the call is finished the state will return to allocated. When the application closes the socket, the state will return to Idle.

The Data state is achieved via successful call progress negotiations. The following is a list of all possible states.

Idle	Signaling	Initiating	Link	Training
EC Negotiating	Data	Resyncing	Fax	Command Escape
Terminating	Port Reset	DSP Reset	Allocated	On Hold

Connection Details

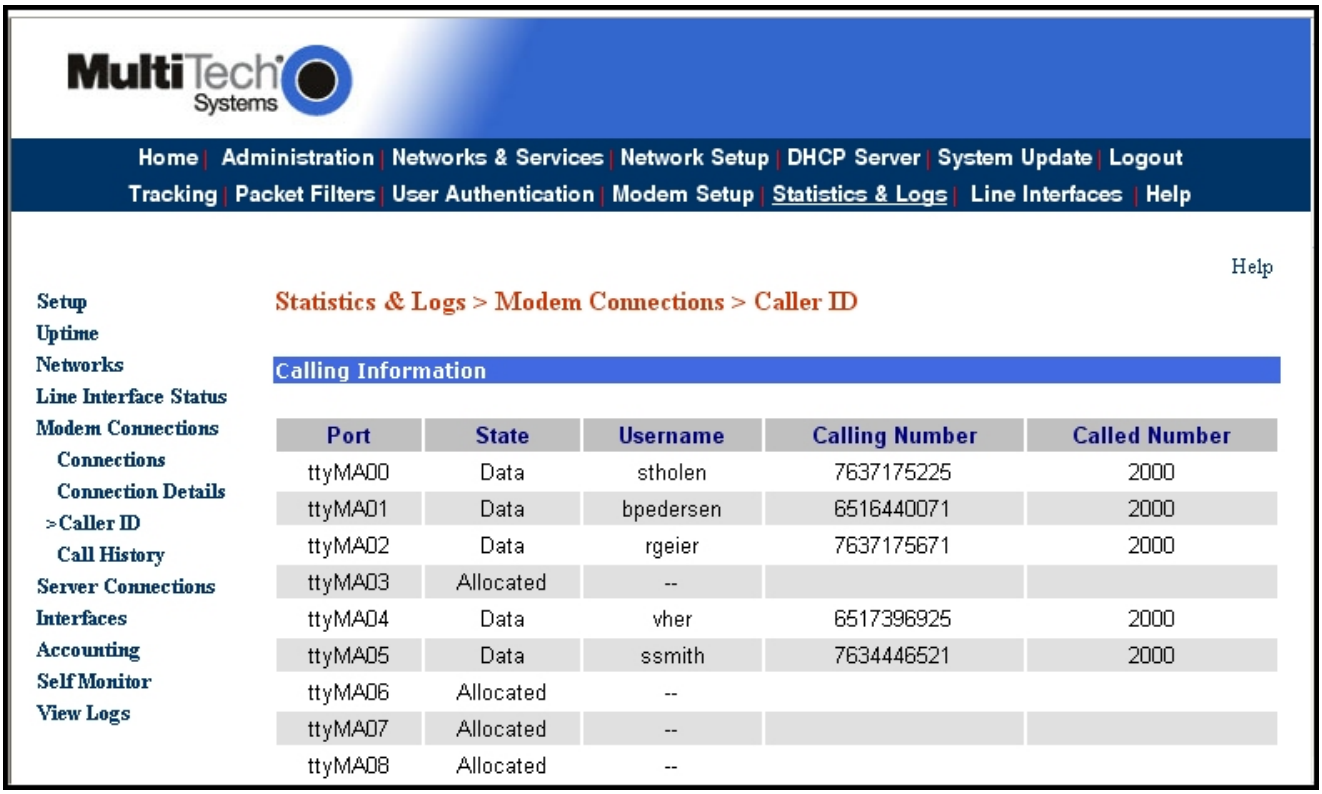
This screen displays the modem protocol and performance details for currently connected ports.



Port	State	Rx / Tx Bit Rate	Link / Compression Protocol	Retrains Initiated / Granted	Renegs Up / Down / Granted
ttyMA00	Data	31200 / 50667	LAPM / V.44 Tx & Rx	0 / 0	0 / 0 / 0
ttyMA01	Data	26400 / 26400	LAPM / V.42bis Tx & Rx	0 / 3	0 / 4 / 9
ttyMA02	Data	31200 / 50667	LAPM / V.42bis Tx & Rx	0 / 0	0 / 0 / 0
ttyMA03	Data	21600 / 34667	LAPM / V.42bis Tx & Rx	0 / 0	0 / 0 / 0
ttyMA04	Data	19200 / 48000	LAPM / V.44 Tx & Rx	0 / 0	0 / 0 / 0
ttyMA05	Data	26400 / 44000	LAPM / V.44 Tx & Rx	0 / 2	0 / 0 / 28
ttyMA06	Allocated				
ttyMA07	Allocated				
ttyMA08	Allocated				
ttyMA09	Data	26400 / 48000	LAPM / V.44 Tx & Rx	0 / 0	0 / 0 / 0
ttyMA10	Allocated				
ttyMA11	Allocated				
ttyMA12	Allocated				
ttyMA13	Allocated				

Calling Information

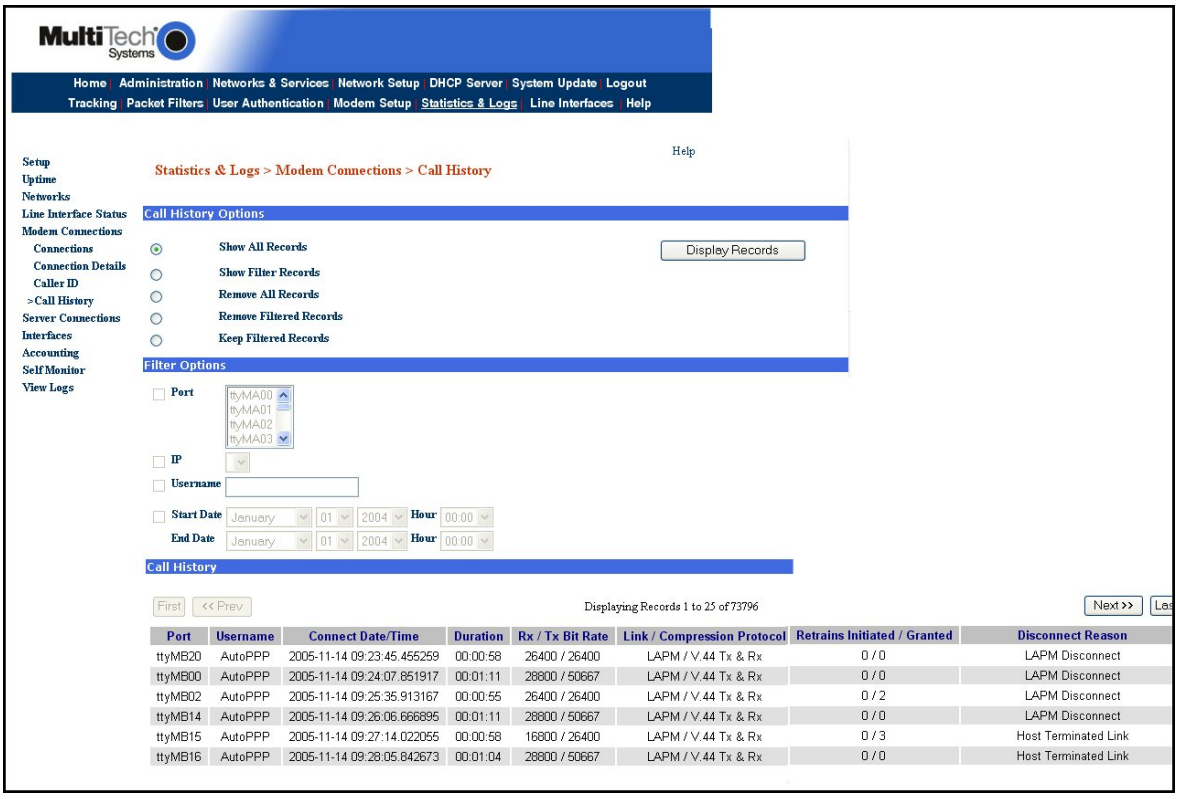
This screen displays the telephone number dialed by the caller and the telephone number of that caller. This information is available when the call is inbound to the MultiAccess and when the line type is PRI (T1PRI or E1 PRI). The exact digits displayed is controlled by Telco's implementation of DNIS (Dialed Number Identification Service) and Caller ID services.



Call History

This screen displays and maintains a call history database. The call history is displayed as a table at the bottom of the page. Available page navigation buttons are Next, Previous, First and Last.

A call (for this database) is defined as an inbound or outbound call with modem carrier being established. Calls that fail to connect are not added to this database. The Call History is maintained in an SQL database. This allows for better search performance on large databases and incorporating the Call History from multiple MultiAccess units into one database.


Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Setup
Uptime
Networks
Line Interface Status
Modem Connections
Connections
Connection Details
Caller ID
>Call History
Server Connections
Interfaces
Accounting
Self Monitor
View Logs
Statistics & Logs > Modem Connections > Call History
Call History Options
Show All Records
Display Records
Show Filter Records
Remove All Records
Remove Filtered Records
Keep Filtered Records
Filter Options
Port
ttyMA00
ttyMA01
ttyMA02
ttyMA03
IP
Username
Start Date
End Date
January
01
2004
Hour
00:00
Call History
First
<< Prev
Displaying Records 1 to 25 of 73796
Next >>
Port
Username
Connect Date/Time
Duration
Rx / Tx Bit Rate
Link / Compression Protocol
Retrains Initiated / Granted
Disconnect Reason
ttyMB20 AutoPPP 2005-11-14 09:23:45.455259 00:00:58 26400 / 26400 LAPM / V.44 Tx & Rx 0 / 0 LAPM Disconnect
ttyMB00 AutoPPP 2005-11-14 09:24:07.851917 00:01:11 28800 / 50667 LAPM / V.44 Tx & Rx 0 / 0 LAPM Disconnect
ttyMB02 AutoPPP 2005-11-14 09:25:35.913167 00:00:55 26400 / 26400 LAPM / V.44 Tx & Rx 0 / 2 LAPM Disconnect
ttyMB14 AutoPPP 2005-11-14 09:26:06.666895 00:01:11 28800 / 50667 LAPM / V.44 Tx & Rx 0 / 0 LAPM Disconnect
ttyMB15 AutoPPP 2005-11-14 09:27:14.022055 00:00:58 16800 / 26400 LAPM / V.44 Tx & Rx 0 / 3 Host Terminated Link
ttyMB16 AutoPPP 2005-11-14 09:28:05.842673 00:01:04 28800 / 50667 LAPM / V.44 Tx & Rx 0 / 0 Host Terminated Link

The default Call History option is to Show All Records (each time the Call History menu is entered) with 25 records (calls) listed per page. To narrow your search of the database, select one of the *Filter Records* choices listed under Call History Options . The Filter Options check boxes will then become selectable.

The Filter Options are by:

Port - The tty port the call was received on.

IP - The IP address of a particular MultiAccess unit (when the Call History database is made up of records from multiple MultiAccess units).

Username - The login name of the dialed in RAS user.

Start Date and Hour (the Hour variable specifies the starting point in time).

End Date and Hour (the Hour variable specifies the final point in time)

You can Show, Remove, or Keep the records specified by the filter options you've chosen. Once you have selected the Filter Options, you can execute the filtering of the database by clicking on the Display Records button.

The Call History Option of Keep Filtered Records means, keep the filtered results and remove all others. Once a call record has been "Removed" it is permanently deleted and can not be brought back.

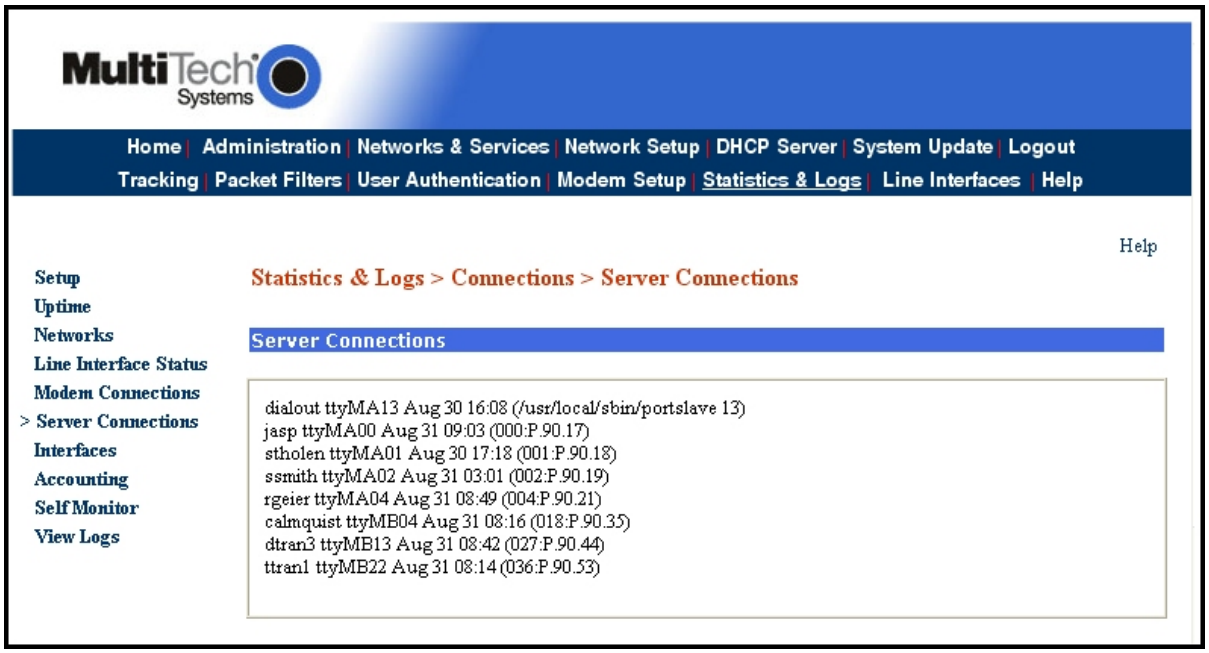
The Call History table contains the following columns displaying details about each call. These columns are selectable, allowing you do organize how the database (all records or filtered records) is displayed.

Port Username Connect Date and Time Duration Rx/Tx Bit Rates
Link Protocol Retrain Occurrences Disconnect Reason

The number of records kept in the database is limited to the amount of system resources available. The time it takes to assemble and display the data structure depends on the number of records in the database, the available system resources and network performance between the MultiAccess and your browser. The larger the database, the longer it takes to display and search the call history. For example we have seen databaseswith approximately 120,000 call records take approximately 120 seconds to display.

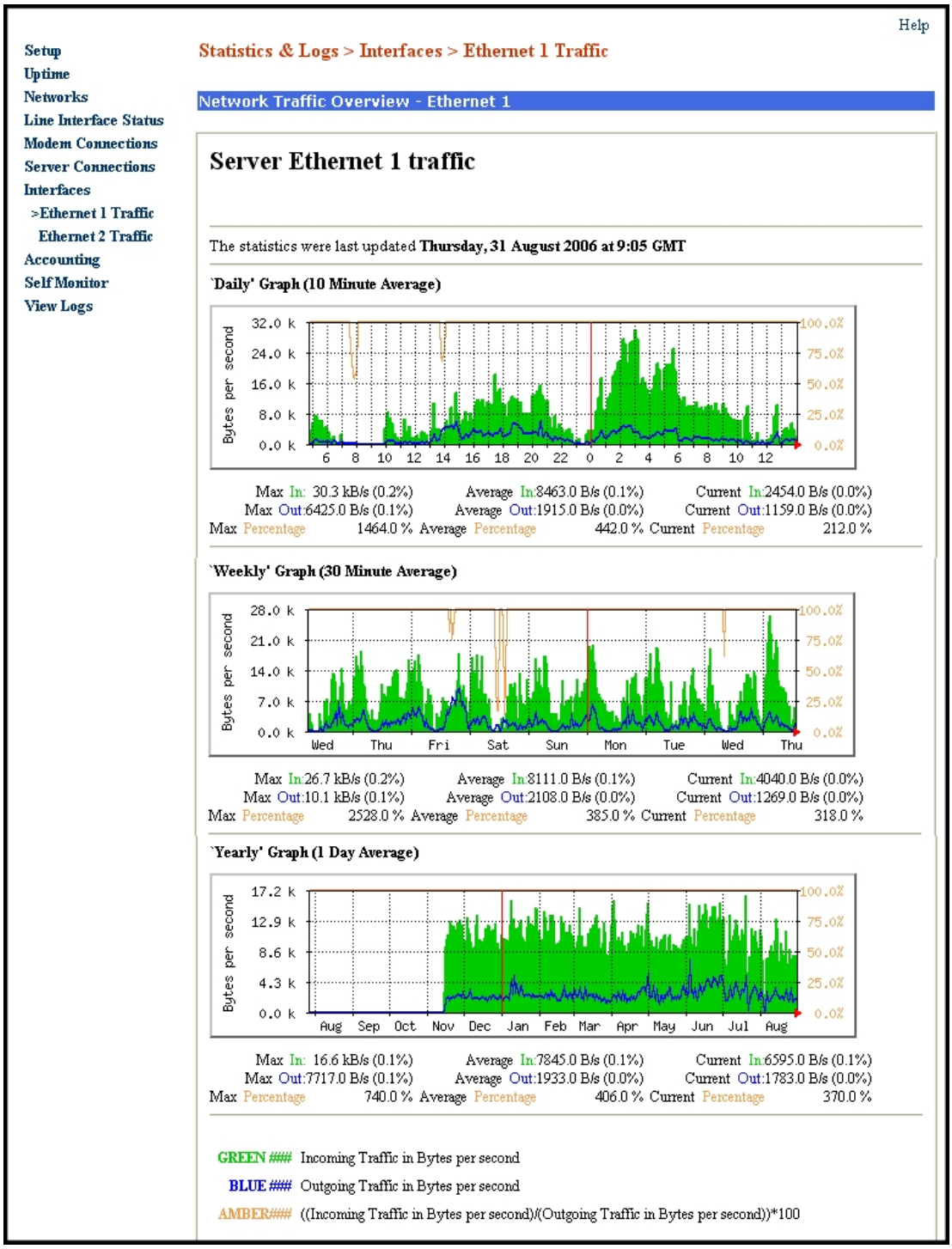
Statistics & Logs > Server Connections

The Server Connections screen displays active command shell PPP sessions and activity.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Setup
Uptime
Networks
Line Interface Status
Modem Connections
> Server Connections
Interfaces
Accounting
Self Monitor
View Logs
Statistics & Logs > Connections > Server Connections
Server Connections
dialout ttyMA13 Aug 30 16:08 (/usr/local/sbin/portslave 13)
jasp ttyMA00 Aug 31 09:03 (000:P.90.17)
stholen ttyMA01 Aug 30 17:18 (001:P.90.18)
ssmith ttyMA02 Aug 31 03:01 (002:P.90.19)
rgeier ttyMA04 Aug 31 08:49 (004:P.90.21)
calmquist ttyMB04 Aug 31 08:16 (018:P.90.35)
dtran3 ttyMB13 Aug 31 08:42 (027:P.90.44)
ttran1 ttyMB22 Aug 31 08:14 (036:P.90.53)

Statistics & Logs > Interfaces

This screen displays graphically the network traffic load on each interface (Ethernet 1 and Ethernet 2) separated by days, weeks, months, and years.

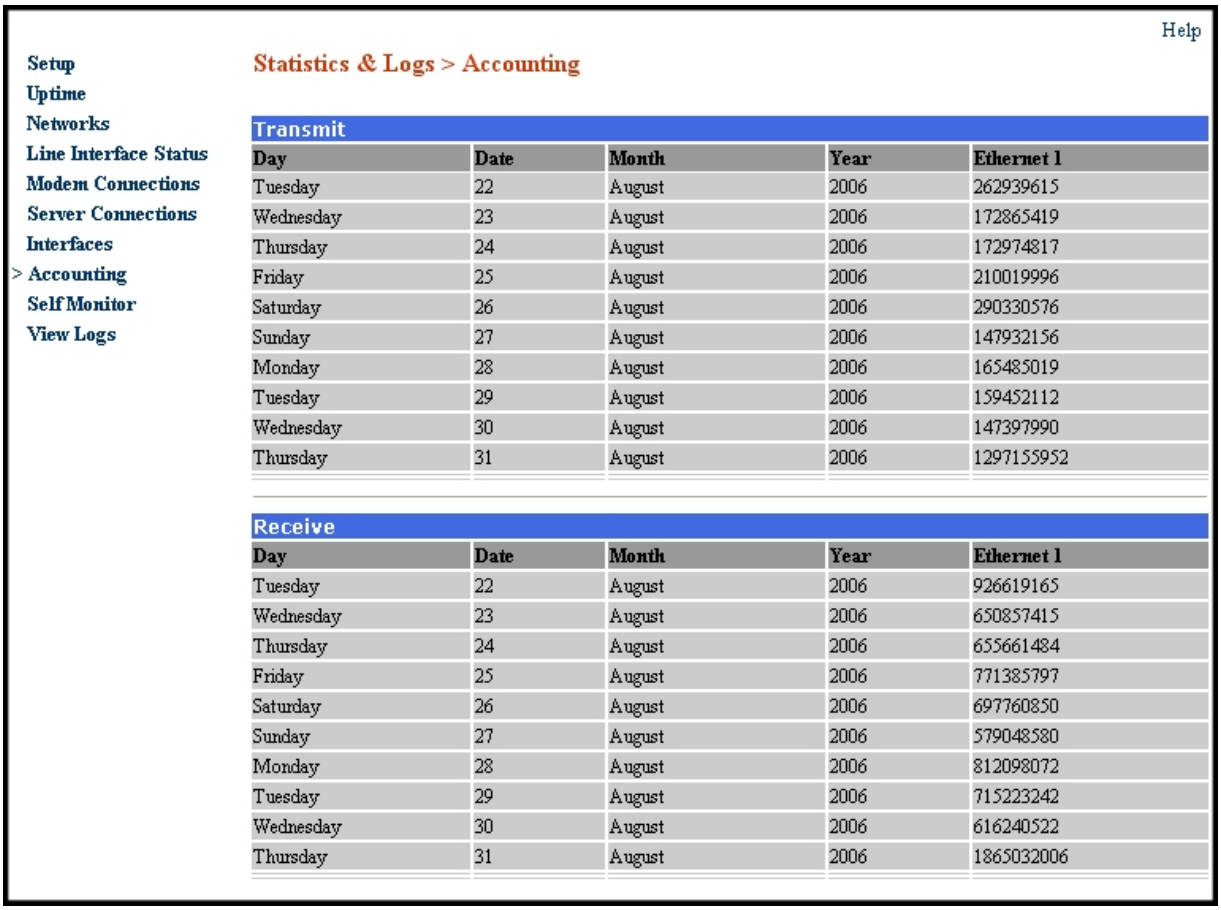

Help
Setup
Uptime
Networks
Line Interface Status
Modem Connections
Server Connections
Interfaces
>Ethernet 1 Traffic
Ethernet 2 Traffic
Accounting
Self Monitor
View Logs
Statistics & Logs > Interfaces > Ethernet 1 Traffic
Network Traffic Overview - Ethernet 1
Server Ethernet 1 traffic
The statistics were last updated Thursday, 31 August 2006 at 9:05 GMT
`Daily' Graph (10 Minute Average)
Bytes per second
32.0 k
24.0 k
16.0 k
8.0 k
0.0 k
100.0%
75.0%
50.0%
25.0%
0.0%
6 8 10 12 14 16 18 20 22 0 2 4 6 8 10 12
Max In: 30.3 kB/s (0.2%) Average In:8463.0 B/s (0.1%) Current In:2454.0 B/s (0.0%)
Max Out:6425.0 B/s (0.1%) Average Out:1915.0 B/s (0.0%) Current Out:1159.0 B/s (0.0%)
Max Percentage 1464.0 % Average Percentage 442.0 % Current Percentage 212.0 %
`Weekly' Graph (30 Minute Average)
Bytes per second
28.0 k
21.0 k
14.0 k
7.0 k
0.0 k
Wed Thu Fri Sat Sun Mon Tue Wed Thu
Max In:26.7 kB/s (0.2%) Average In:8111.0 B/s (0.1%) Current In:4040.0 B/s (0.0%)
Max Out:10.1 kB/s (0.1%) Average Out:2108.0 B/s (0.0%) Current Out:1269.0 B/s (0.0%)
Max Percentage 2528.0 % Average Percentage 385.0 % Current Percentage 318.0 %
`Yearly' Graph (1 Day Average)
Bytes per second
17.2 k
12.9 k
8.6 k
4.3 k
0.0 k
Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug
Max In: 16.6 kB/s (0.1%) Average In:7845.0 B/s (0.1%) Current In:6595.0 B/s (0.1%)
Max Out:7717.0 B/s (0.1%) Average Out:1933.0 B/s (0.0%) Current Out:1783.0 B/s (0.0%)
Max Percentage 740.0 % Average Percentage 406.0 % Current Percentage 370.0 %
GREEN ### Incoming Traffic in Bytes per second
BLUE ### Outgoing Traffic in Bytes per second
AMBER### ((Incoming Traffic in Bytes per second)/(Outgoing Traffic in Bytes per second))*100

Ethernet 1 Traffic – Ethernet 1 traffic is displayed by default.

Ethernet 2 Traffic – Click on Ethernet 2 traffic to graphically display the traffic on Ethernet 2.

Statistics & Logs > Accounting

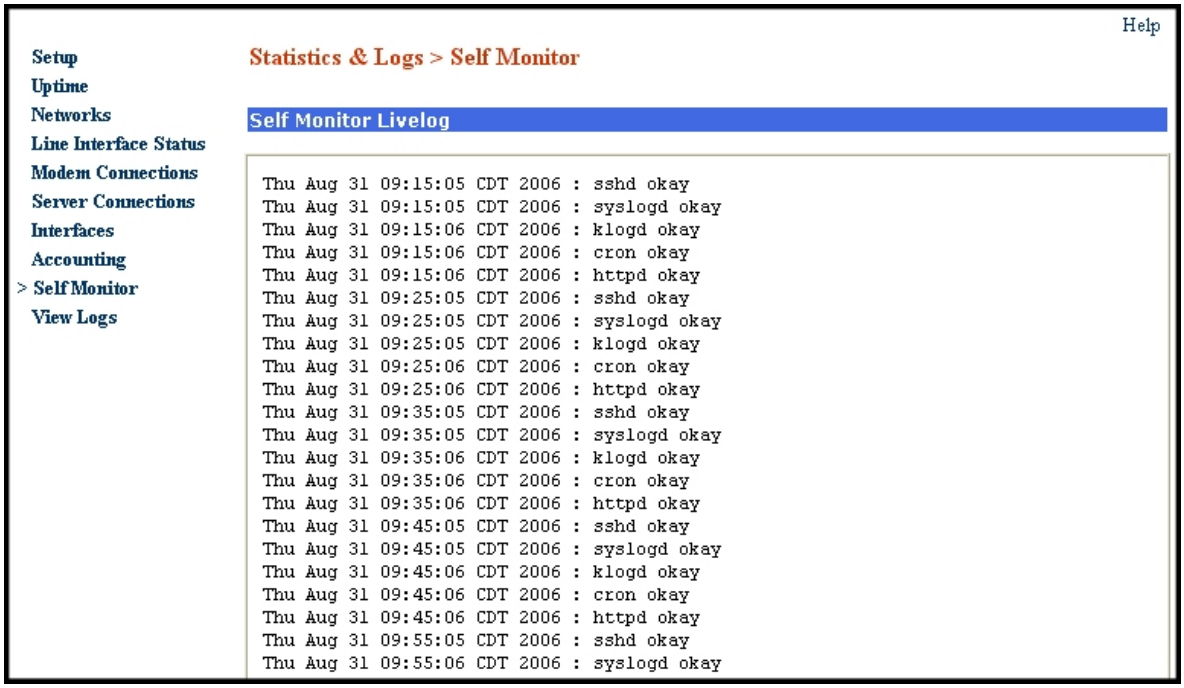
This screen displays daily byte totals of network traffic transferred through each MultiAccess Ethernet interface. This network traffic Accounting feature is off by default. Use the Tracking> Accounting menu to enable accounting per Ethernet interface.



Each day's total is separated by the amount transmitted per Ethernet interface and received per Ethernet interface (transmit is from the MultiAccess to the LAN, Receive is from the LAN to the MultiAccess). The length of each Ethernet Frame transmitted (or received) by the MultiAccess is added up to achieve the byte total. One Ethernet frame (packet) contains one IP packet of a various length, hence so is the length of each Ethernet packet. These totals can be helpful if your ISP charges based on the volume of Internet traffic.

Statistics & Logs > Self Monitor

The Self Monitoring function informs the administrator when important internal processes have stopped running. The Self Monitoring function will check every 10 minutes to see if certain process are running. If a particular process is no longer running, it will send an email stating which process is not running and is trying to be restarted.


Help
Setup
Uptime
Networks
Line Interface Status
Modem Connections
Server Connections
Interfaces
Accounting
> Self Monitor
View Logs
Statistics & Logs > Self Monitor
Self Monitor Livelog
Thu Aug 31 09:15:05 CDT 2006 : sshd okay
Thu Aug 31 09:15:05 CDT 2006 : syslogd okay
Thu Aug 31 09:15:06 CDT 2006 : klogd okay
Thu Aug 31 09:15:06 CDT 2006 : cron okay
Thu Aug 31 09:15:06 CDT 2006 : httpd okay
Thu Aug 31 09:25:05 CDT 2006 : sshd okay
Thu Aug 31 09:25:05 CDT 2006 : syslogd okay
Thu Aug 31 09:25:05 CDT 2006 : klogd okay
Thu Aug 31 09:25:06 CDT 2006 : cron okay
Thu Aug 31 09:25:06 CDT 2006 : httpd okay
Thu Aug 31 09:35:05 CDT 2006 : sshd okay
Thu Aug 31 09:35:05 CDT 2006 : syslogd okay
Thu Aug 31 09:35:06 CDT 2006 : klogd okay
Thu Aug 31 09:35:06 CDT 2006 : cron okay
Thu Aug 31 09:35:06 CDT 2006 : httpd okay
Thu Aug 31 09:45:05 CDT 2006 : sshd okay
Thu Aug 31 09:45:05 CDT 2006 : syslogd okay
Thu Aug 31 09:45:06 CDT 2006 : klogd okay
Thu Aug 31 09:45:06 CDT 2006 : cron okay
Thu Aug 31 09:45:06 CDT 2006 : httpd okay
Thu Aug 31 09:55:05 CDT 2006 : sshd okay
Thu Aug 31 09:55:06 CDT 2006 : syslogd okay

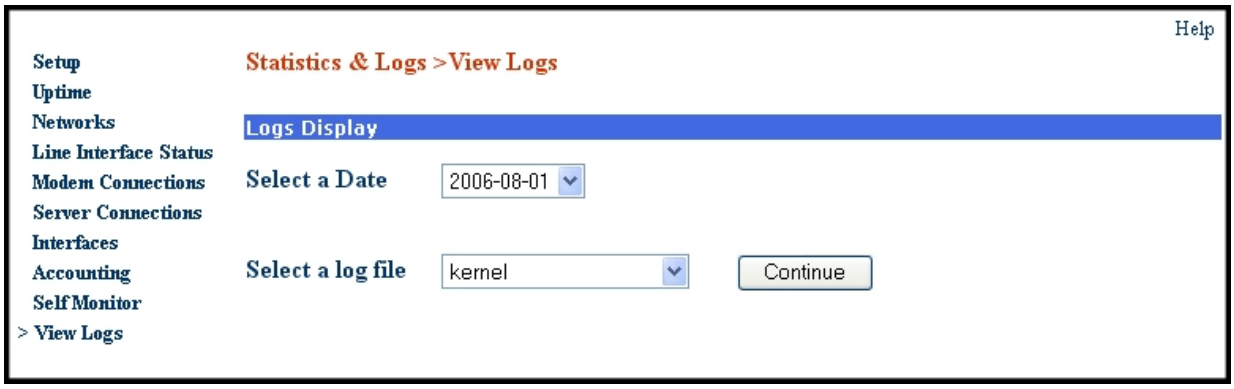
How to Add, Edit, or Delete Email Addresses for Self Monitoring:

1. Open the **Administration > System Setup** screen. The current email addresses for informing the administrator of important events are listed in the second window of the **Notification** entry menu.
2. Edit or delete existing email addresses or add new email addresses, and then click **Save**.

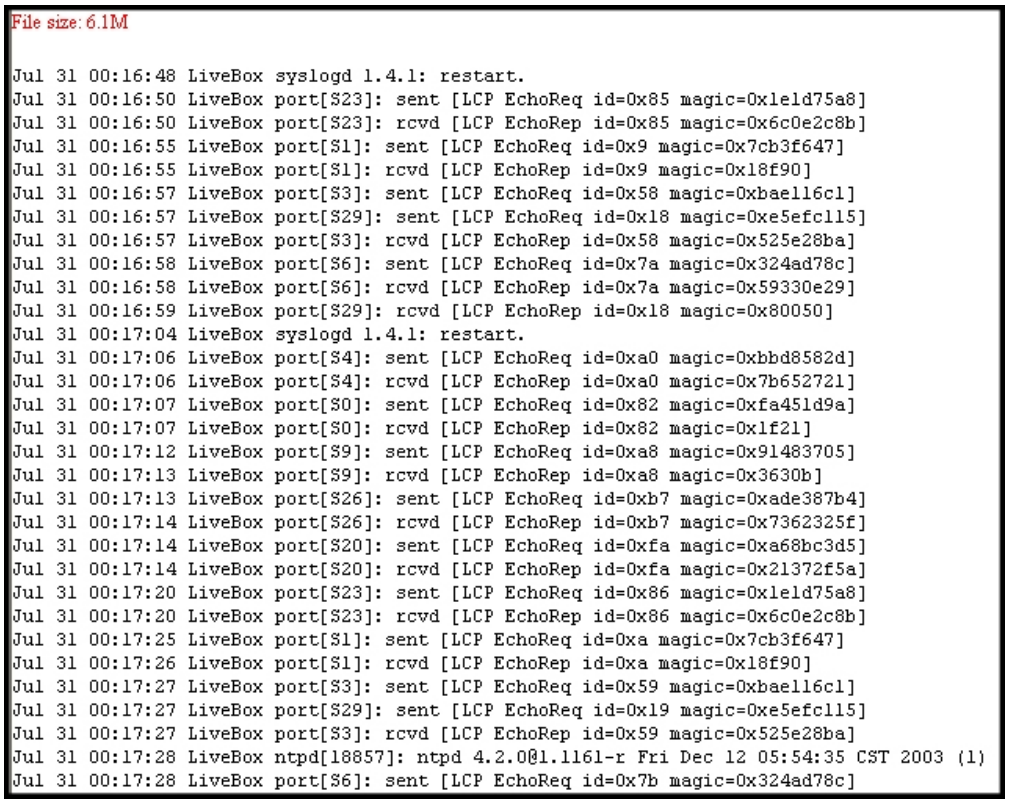
   Note: By clicking the **Delete** button, the email addresses marked in the select window are immediately deleted without further notice. At least one email address has to be entered. The last email address listed cannot be deleted.

Statistics & Logs > View Logs

This screen allows you to display, download, and search a pattern in various logs maintained by the MultiAccess.



Select a Date and log file type from the pull down window, and click Continue. A detailed log file is displayed.



```
File size: 6.1M

Jul 31 00:16:48 LiveBox syslogd 1.4.1: restart.
Jul 31 00:16:50 LiveBox port[S23]: sent [LCP EchoReq id=0x85 magic=0x1e1d75a8]
Jul 31 00:16:50 LiveBox port[S23]: rcvd [LCP EchoRep id=0x85 magic=0x6c0e2c8b]
Jul 31 00:16:55 LiveBox port[S1]: sent [LCP EchoReq id=0x9 magic=0x7cb3f647]
Jul 31 00:16:55 LiveBox port[S1]: rcvd [LCP EchoRep id=0x9 magic=0x18f90]
Jul 31 00:16:57 LiveBox port[S3]: sent [LCP EchoReq id=0x58 magic=0xbae116c1]
Jul 31 00:16:57 LiveBox port[S29]: sent [LCP EchoReq id=0x18 magic=0xe5efc115]
Jul 31 00:16:57 LiveBox port[S3]: rcvd [LCP EchoRep id=0x58 magic=0x525e28ba]
Jul 31 00:16:58 LiveBox port[S6]: sent [LCP EchoReq id=0x7a magic=0x324ad78c]
Jul 31 00:16:58 LiveBox port[S6]: rcvd [LCP EchoRep id=0x7a magic=0x59330e29]
Jul 31 00:16:59 LiveBox port[S29]: rcvd [LCP EchoRep id=0x18 magic=0x80050]
Jul 31 00:17:04 LiveBox syslogd 1.4.1: restart.
Jul 31 00:17:06 LiveBox port[S4]: sent [LCP EchoReq id=0xa0 magic=0xbbd8582d]
Jul 31 00:17:06 LiveBox port[S4]: rcvd [LCP EchoRep id=0xa0 magic=0x7b652721]
Jul 31 00:17:07 LiveBox port[S0]: sent [LCP EchoReq id=0x82 magic=0xfa451d9a]
Jul 31 00:17:07 LiveBox port[S0]: rcvd [LCP EchoRep id=0x82 magic=0x1f21]
Jul 31 00:17:12 LiveBox port[S9]: sent [LCP EchoReq id=0xa8 magic=0x91483705]
Jul 31 00:17:13 LiveBox port[S9]: rcvd [LCP EchoRep id=0xa8 magic=0x3630b]
Jul 31 00:17:13 LiveBox port[S26]: sent [LCP EchoReq id=0xb7 magic=0xade387b4]
Jul 31 00:17:14 LiveBox port[S26]: rcvd [LCP EchoRep id=0xb7 magic=0x7362325f]
Jul 31 00:17:14 LiveBox port[S20]: sent [LCP EchoReq id=0xfa magic=0xa68bc3d5]
Jul 31 00:17:14 LiveBox port[S20]: rcvd [LCP EchoRep id=0xfa magic=0x21372f5a]
Jul 31 00:17:20 LiveBox port[S23]: sent [LCP EchoReq id=0x86 magic=0x1e1d75a8]
Jul 31 00:17:20 LiveBox port[S23]: rcvd [LCP EchoRep id=0x86 magic=0x6c0e2c8b]
Jul 31 00:17:25 LiveBox port[S1]: sent [LCP EchoReq id=0xa magic=0x7cb3f647]
Jul 31 00:17:26 LiveBox port[S1]: rcvd [LCP EchoRep id=0xa magic=0x18f90]
Jul 31 00:17:27 LiveBox port[S3]: sent [LCP EchoReq id=0x59 magic=0xbae116c1]
Jul 31 00:17:27 LiveBox port[S29]: sent [LCP EchoReq id=0x19 magic=0xe5efc115]
Jul 31 00:17:27 LiveBox port[S3]: rcvd [LCP EchoRep id=0x59 magic=0x525e28ba]
Jul 31 00:17:28 LiveBox ntpd[18857]: ntpd 4.2.0@1.1161-r Fri Dec 12 05:54:35 CST 2003 (1)
Jul 31 00:17:28 LiveBox port[S6]: sent [LCP EchoReq id=0x7b magic=0x324ad78c]
```

The type of log file selected effects the behavior and results of the time and date options.

When the log file type is kernel, the time option specifies the ending point you are interested in. All logs will contain entries that start just after midnight (the zero hour) on the date selected and end at the time selected. The time selection of “latest” is only available when the date selected is today’s current date. Please note this exception, the time selection of “00:00” will result in viewing the previous day’s entire log.

When the log file type is Self Monitor and the selected date is **not** today’s date, due to the nature of how the logs are maintained, there is only one time choice available and will result in viewing the entire log for the day previous to what is specified. When the date selected is the current date (today’s date), two choices become available in the time drop down field (“latest” and “00:16”). The selection of “latest” will result in viewing all entries for today. The selection of “00:16” will result in viewing the previous day’s log.

Line Interfaces

The Line Interfaces menu is used to configure the active (enabled) digital communication line interfaces within the MultiAccess. All MultiAccess units come with four built in digital line interfaces. The first line interface is enabled by default because all units come pre-installed with one 30-modem module. The three remaining line interfaces can be activated as needed by installing an MA30EXP port expansion module into the corresponding position, increasing the number of modems within the unit.

The line interfaces can be set to either E1 or T1 digital line types via software control, however all interfaces within the unit must be set to the same basic type (all must be T1 or all must be E1). After changing from one to the other, the MultiAccess requires a reboot.

The following statements attempt to summarize, in the simplest terms, certain digital carrier technology, T1 and E1 lines, in relationship to the MultiAccess.

T1 and E1 signals are made up of multiple protocols running at multiple levels. Layer 1 refers to the framed signal physically transmitted and received on the wires (transport layer). Layer 2, runs a signaling, or messaging protocol that is responsible for communicating, signaling, the establishment of a call between end points. Layer 2 takes place within certain resources, areas, of the Layer 1 signal.

E1 Digital Line

E1 layer 1- a 32 channel (plus overhead) signal at 2.048 Mbit/s

E1 layer 2 - the MultiAccess supports only one type of E1 signaling method, ISDN_PRI (a.k.a. CCS)

Other methods exist (Like R2 Digital and R2MF), but these are not supported.

T1 Digital Line

T1 Layer 1 - a 24 channel (plus overhead) signal at 1.544 Mbit/s

T1 Layer 2 - the MultiAccess supports two methods of T1 signaling, ISDN_PRI and RBS

RBS (Robbed Bit Signaling) - CAS (Channel Associated Signaling)

ISDN_PRI - CCS (Common Channel Signaling)

Line Interfaces > Line x Setup

The Line Setup screen is made up of two fields, Current Setup (which displays the saved and active settings) and Setup. The contents of the Current Setup field will not change until after the setup parameters have been properly loaded. The Setup field is used to load the parameters into the line interface. The parameters you select should match the parameters of the digital communication line provided by your Telco.

The proper loading sequence is:

- Select the desired Line Type and wait for the screen to refresh (the available menu options will change based on the selected line type).
- Change any of the remaining options as needed.
- Click on the Save button and wait for the screen to refresh. The Send button will now be active.
- Click the Send button and wait for the screen to refresh (this takes approximately 45 seconds).
- Now the Current Setup field will reflect the new settings.

Line Type

Three selections are available, T1-RBS, T1-PRI and E1-PRI. Units leave the factory set to E1-PRI. Line Interfaces that are activated in the field (when an MA30EXP port expansion module is installed) will default to T1-RBS. Whenever the line type setting is changed form E1-PRI to a T1 choice (or from a T1 choice to E1-PRI), after saving and sending the configuration change, the unit MUST be restarted. However, changing from T1-RBS to T1-PRI or changing any other parameter (for example the Framing Format or Line Build Out) does NOT require a system reboot.

Tl PRI

A T1 line implementing PRI signaling (commonly referred to as a PRI line). PRI (ISDN) signaling is a layer 2 protocol. T1-PRI (23B+D) uses channels 1 through 23 to Bear (carry) the calls (1 call per channel) and uses the 24th channel (D Channel) as the signaling channel. The D-channel is used to send Call Setup and Call Progress messages between Telco's central office switch and the MultiAccess (premise equipment). PRI Signaling allows for analog calls or digital calls to be made per channel. When this line type is selected, 23 modems will be made available to this particular interface (ttyM*X*00 through ttyM*X*22, with *x* being a variable A through D, depending if the Line Interface is 1 through 4).

T1 RBS

A T1 line implementing Robbed Bit Signaling (commonly referred to as a standard T1 line). All 24 channels are Bearer channels, supporting analog calls only. The signaling of calls between the central office equipment (FXO side) and the MultiAccess (FXS side) is done within each channel using the AB bits and DTMF tones. When this line type is selected, 24 modems will be made available to this particular interface (ttyMX00 through ttyMX23 with *x* being a variable A through D, depending if the Line Interface is 1 through 4).

E1 PRI

An E1 line implementing PRI signaling. PRI (ISDN) signaling is a layer 2 protocol. E1-PRI has 32 channels numbered 0 through 31. Channel zero is used as the framing channel, channels 1 through 15 and 17 through 31 are the bearer channels and channel 16 is the D-Channel (call signaling channel). The D-channel is used to send Call Setup and Call Progress messages between Telco's central office switch and the MultiAccess (premise equipment). PRI Signaling allows for analog calls or digital calls to be made per channel. When this line type is selected, 30 modems will be made available to this particular interface (ttyM*X*00 through ttyM*X*29, with *x* being a variable A through D depending if the Line Interface is 1 through 4).

Interfaces > Line x Setup> T1 RBS

The Line Setup screen is made up of two fields, Current Setup (which displays the saved and active settings) and Setup. The contents of the Current Setup field will not change until after the setup parameters have been properly loaded. The Setup field is used to load the parameters into the line interface. The parameters you select should match the parameters of the digital communication line provided by your Telco.

The proper loading sequence is:

- Select the desired Line Type and wait for the screen to refresh (the available menu options will change based on the selected line type).
- Change any of the remaining options as needed.
- Click on the Save button and wait for the screen to refresh. The Send button will now be active.
- Click the Send button and wait for the screen to refresh (this takes approximately 45 seconds).
- Now the Current Setup field will reflect the new settings.

MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
> Line 1 Setup
Line 2 Setup
Line 3 Setup
Line 4 Setup
Line Interfaces > Line 1 Setup
Current Setup
Line Type T1 RBS
Framing Format Extended Super Frame (ESF) with Error Correction
Line Code Binary 8 Zero Substitution (B8ZS)
Receive Sensitivity Short Haul Mode (-10db)
FXS Signaling Method E&M Wink Start
Line Build Out - 0.0dB
Remote (Yellow) Alarm Format 0
Wink High Time 220
Pre Wink Time 220
After Wink Time 500
Voice Channel Encoding µ-law
T1 Setup
Line Type T1 RBS
Framing Format EXTENDED SUPER FRAME (ESF) WITH ERROR CORRECTION
Line Code BINARY 8 ZERO SUBSTITUTION (B8ZS)
Receive Sensitivity SHORT HAUL MODE (-10DB)
FXS Signaling Method E&M WINK START
Line Build Out - 0.0DB
Remote (Yellow) Alarm Format PATTERN \1111 1111 0000 0000...\ IN DATA LINK CHANNEL
Wink High Time (ms) 220
Pre Wink Time (ms) 220
After Wink Time (ms) 500
Voice Channel Encoding µ-LAW
Save
Send

Line Type

Three selections are available, T1-RBS, T1-PRI and E1-PRI. Units leave the factory set to E1-PRI. Line Interfaces that are activated in the field (when an MA30EXP port expansion module is installed) will default to T1-RBS. Whenever the line type setting is changed form E1-PRI to a T1 choice (or from a T1 choice to E1-PRI), after saving and sending the configuration change, the unit MUST be restarted. However, changing from T1-RBS to T1-PRI or changing any other parameter (for example the Framing Format or the Line Build Out) does NOT require a system reboot.

Framing Format

The Framing Format parameter is a layer 1 parameter used to construct & identify the basic signal transmitted and received. The Line Type selection dictates the available formats.

When the line type is T1, your choices are:

- Extended Super Frame (ESF),
- Extended Super Frame (ESF) with Error Correction,
- 12 Frame MultiFrame (F12), - *same as industry D4 Super Frame(SF)*
- 4 Frame MultiFrame (F4),
- 72 Frame MultiFrame - Remote Switch Mode (F72)

Note: The majority of T1 lines in North America now implement ESF framing with Error Correction (CRC4\6 on), however commonly referred to as just “ESF”.

Line Code

The Line Code parameter is a layer 1 technique used to identify and control the ones and zeros of the data pattern. T1 line codes are derived from the AMI (Alternate Mark Inversion) bi-polar technique. A voltage (pulse) on the digital line represents a binary one. No voltage represents a binary zero. The line code says each binary one must be of the opposite polarity with respect to the previous one (voltage alternating in polarity - the essence of a bipolar signal). The Line Type selection dictates the available Line Code choices.

When the line type is T1, your choices are:

Alternate Mark Inversion (AMI)

Line code is a bipolar coding scheme in which successive ones alternate in polarity. Successive ones of the same polarity are bipolar violations (BPV errors). BPVs and too many consecutive zeros are conditions that cause signal degradation. AMI line code requires user data to contain enough binary ones to maintain 1s density (signal integrity). The 1s Density rule is, in every 24 bits of information to be transmitted, there must be at least 3 ones (pulses) and that no more than 15 zeros can be transmitted consecutively.

Binary 8 Zero Substitution (B8ZS)

B8ZS (Binary 8 Zero Substitution). This line code is the same as AMI, except for when user data does not contain enough binary ones to maintain the “1s Density” rule). A “user” data stream of 16 consecutive zeros (to be transmitted) will be replaced with a B8ZS pattern (a pattern that contains a specific sequence of bipolar violations). The receiving end of this transmission will also be set to B8ZS line code and so when it recovers the specific pattern of violations, it will replace it with a string of zeros (transparently passing the data up to the receiving user as originally intended).

Receive Sensitivity

This layer 1 parameter configures (tunes) the interface’s receiver circuit. There are two choices to select from, Short Haul Mode (-10db) and Long Haul Mode (-36 dB).

T1 signals are full duplex. A T1 digital interface generates and transmits a signal onto the line, while at the same time it receives and recovers a signal from the line.

Short Haul Mode (-10db)

Setting the receive sensitivity to Short Haul Mode means the MultiAccess receiver expects the size of the incoming signal to be between 0db and -10db. If the incoming signal is greater than 0db or if it’s smaller than -10 dB, the interface will indicate a Red Alarm condition.

Long Haul Mode (-36db)

Setting the receive sensitivity to Long Haul Mode means the MultiAccess receiver expects the size of the incoming signal to be between -10db and -36db. If the incoming signal is smaller than -36 dB, the interface will not be able to recover it and will indicate a Red Alarm condition. If the incoming signal is greater than -10 dB, depending on many variables (wave shape, jitter, dB level, cable quality, EMI, etc) erratic communication, bit errors and other problems may or may not result.

FXS Signaling Method

This parameter only applies (and is made available) when the Line Type is set to T1-RBS and selects the specific RBS method of signaling. Your choices are; E&M Wink Start, E&M Immediate Start, Ground Start and Loop Start.

T1 lines implementing RBS signaling use the state of the AB bits to determine and establish Call Progress. The state of the AB bits (00 or 01 or 10 or 11) take on different meanings when this parameter changes. For example, when set to E&M Immediate Start 00 means idle (on hook) but when set to Loop Start 01 means idle.

The Loop Start and Ground Start protocols implement an FXO to FXS relationship. Equipment at one end must be in FXO mode while the equipment at the other end must be in FXS mode. The MultiAccess performs FXS side operation only, so the Central Office equipment (or private PBX type equipment on your premise) at the other end of the T1 link must be set to FXO. FXS verses FXO does not apply when the signaling protocol is E&M.

For Example:

If you're connecting the MultiAccess to a T1 line from Telco and their central office switch is set to FXO-**Loop** Start and the MultiAccess is set to FXS-**Ground** Start, the call signaling will fail because they are not using the same **protocol** (both need to be Ground Start or both need to be Loop Start).

If You're connecting the MultiAccess to a T1 line that comes from a PBX system on your premise and it's set to FXS-Loop Start and the MultiAccess is also set to FXS-Loop Start, the call signaling will fail because they are not maintaining the FXO to FXS relationship.

Line Build Out (LBO)

This layer 1 parameter dictates the physical size (decibel level) of the T1 signal being transmitted by the MultiAccess. Your choices are 0dB, -7.5dB, -15 dB & -22.5 dB. 0dB is the largest size signal the MultiAccess can transmit.

There are a number of variables as to when the Line Build Out setting should be changed. The primary factors are, cable length, gauge and quality (twists per inch and shielding), and what size signal does the equipment opposite to the MultiAccess want to receive from the MultiAccess. As the signal travels down the cable it attenuates (becomes smaller and it's wave shape starts to change) - what size will it be at the other end of the cable?

If the receiving equipment (for example a T1 card in a PBX on your premise) is connected to the MultiAccess with a 6 foot cable, having the MultiAccess transmit at 0dB may be too hot (too large) of a signal for that device to receive, so setting the Line Build Out to -15dB may be more appropriate.

Remote (Yellow) Alarm Format

This parameter only applies (and is made available) when the Line Type is set to T1. This option dictates what pattern is transmitted when the MultiAccess is to send a Yellow Alarm signal. This also dictates what pattern is detected (looked for) in the incoming (recovered) T1 signal. The default format is a 16 bit pattern of 8 ones followed by 8 zeros, which is sent in the Facility Data Link channel of an ESF framed T1 signal. When the framing format is set to F12 (D4 Super Frame), this option should be set to the pattern of "bit2 in every channel = zero".

Wink Times (High, Pre & After)

Wink times only apply and become changeable when the Line Type is set to T1-RBS and the FXS Signaling method is set to E&M Wink Start.

The AB bits transmitted by the MultiAccess will “wink” back to the Central Office upon detection of an inbound call. The sequence of events is as follows:

- No call = both sides (Telco equipment and MultiAccess) indicate idle (transmit 00).
- Telco indicates off hook (transmits 11 to MultiAccess).
- MultiAccess receives 11 (off hook) from Telco, causing the MultiAccess modem to indicate Ring detected.
- MultiAccess waits the duration of the “Pre Wink Time”, then transmits 11 for the duration of “Wink High Time” (winks), then returns to indicating idle (transmits 00) for the duration of the “After Wink Time”.
- When the After Wink Time expires, the MultiAccess continues to indicate on hook (transmit 00) until the MultiAccess modem is instructed to answer.
- When instructed to answer the MultiAccess indicates off hook (transmits 11) until the completion of the modem call.

When the MultiAccess originates a call, it waits to see a wink from the Central Office before it transmits the DTMF digits. The sequence of events is as follows:

- No call = both sides (Telco equipment and MultiAccess) indicate idle (transmit 00).
- MultiAccess modem is instructed to dail.
- MultiAccess indicates off hook (transmits 11 to Telco).
- Telco winks back (in the same fashion as the MultiAccess did in the previous example).
- After the MultiAccess detects the wink, it transmits the DTMF digits (in the voice\B_Channel).
- The MultiAccess modem then listens into the channel (for a busy signal from Telco) and at the same time watches the state of the incoming AB bits.
- If a busy signal is not heard and the destination picks up, Telco indicates off hook (the incoming bits change to 11), the modem proceeds with the call and listens for answer tones from the answering side modem. Telco indicates off hook until the answering side hangs up.
- If a busy signal is not heard and the incoming bits never indicate off hook, the modem will declare No Answer after it’s S7 timer expeires.
- When the call is terminated or completed, the MultiAccess will transmit on hook (00) until the start of the next call.

Voice Channel Encoding

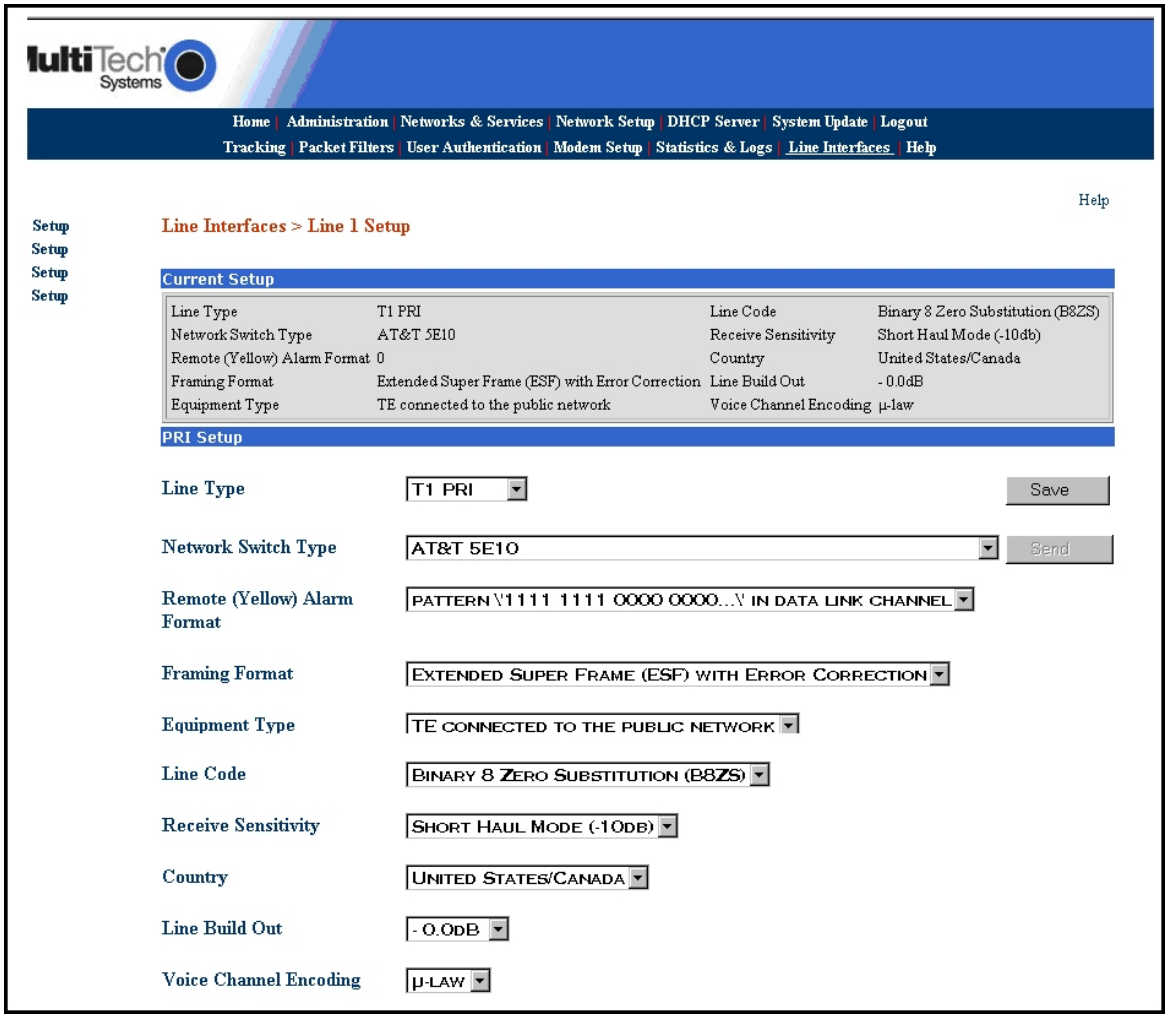
This parameter automatically follows the Line Type selection, however the user can change it from it’s defaults. When the line type is set to E1 the PCM rule (Voice Channel Encoding) will be set to A-law. When the line type is set to T1 this option will be set to u-law. The ability to change this setting independent of the line type allows for flexibility in privately controlled closed circuit networks.

Line Interfaces > Line x Setup > T1 PRI

The Line Setup screen is made up of two fields, Current Setup (which displays the saved, active, settings) and Setup. The contents of the Current Setup field will not change until after the setup parameters have been properly loaded. The Setup field is used to load the parameters into the line interface. The parameters you select should match the parameters of the digital communication line provided by Telco.

The proper loading sequence is:

- Select the desired Line Type and wait for the screen to refresh (the available menu options will change based on the selected line type).
- Change any of the remaining options as needed.
- Click on the Save button and wait for the screen to refresh (the Send button will now be active).
- Click the Send button and wait for the screen to refresh (this takes approximately 45 seconds).
- Now the Current Setup field will reflect the new settings.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
Setup
Setup
Setup
Setup
Line Interfaces > Line 1 Setup
Current Setup
Line Type T1 PRI
Line Code Binary 8 Zero Substitution (B8ZS)
Network Switch Type AT&T 5E10
Receive Sensitivity Short Haul Mode (-10db)
Remote (Yellow) Alarm Format 0
Country United States/Canada
Framing Format Extended Super Frame (ESF) with Error Correction
Line Build Out - 0.0dB
Equipment Type TE connected to the public network
Voice Channel Encoding µ-law
PRI Setup
Line Type
T1 PRI
Save
Network Switch Type
AT&T 5E10
Send
Remote (Yellow) Alarm Format
PATTERN \'1111 1111 0000 0000...\' IN DATA LINK CHANNEL
Framing Format
EXTENDED SUPER FRAME (ESF) WITH ERROR CORRECTION
Equipment Type
TE CONNECTED TO THE PUBLIC NETWORK
Line Code
BINARY 8 ZERO SUBSTITUTION (B8ZS)
Receive Sensitivity
SHORT HAUL MODE (-10DB)
Country
UNITED STATES/CANADA
Line Build Out
- 0.0DB
Voice Channel Encoding
µ-LAW

Line Type

Three selections are available, T1-RBS, T1-PRI and E1-PRI. Units leave the factory set to E1-PRI. Line Interfaces that are activated in the field (when an MA30EXP port expansion module is installed) will default to T1-RBS. Whenever the line type setting is changed form E1-PRI to a T1 choice (or from a T1 choice to E1-PRI), after saving and sending the configuration change, the unit MUST be restarted. However, changing from T1-RBS to T1-PRI or changing any other parameter (for example the Framing Format or the Line Build Out) does NOT require a system reboot.

Network Switch Type

This parameter only applies (and is made available) when the line type implements PRI_ISDN signaling (T1-PRI). This parameter selects the specific messaging protocol that runs within the D_Channel between the Central Office switch and the MultiAccess.

Remote (Yellow) Alarm Format

This parameter only applies (and is made available) when the Line Type is set to T1. This option dictates what pattern is transmitted when the MultiAccess is to send a Yellow Alarm signal. This also dictates what pattern is detected (looked for) in the incoming (recovered) T1 signal. The default format is a 16 bit pattern of 8 ones followed by 8 zeros, which is sent in the Facility Data Link channel of an ESF framed T1 signal. When the framing format is set to F12 (D4 Super Frame), this option should be set to the pattern of "bit2 in every channel = zero".

Framing Format

The Framing Format parameter is a layer 1 parameter used to construct & identify the basic signal transmitted and received. The Line Type selection dictates the available formats.

When the line type is T1, your choices are:

- Extended Super Frame (ESF),
- Extended Super Frame (ESF) with Error Correction,
- 12 Frame MultiFrame (F12), - same as industry D4 Super Frame (SF),
- 4 Frame MultiFrame (F4),
- 72 Frame MultiFrame – Remote Switch Mode (F72)

Note: The majority of T1 lines in North America now implement ESF framing with Error Correction (CRC4\6 on), however commonly referred to as just "ESF".

Equipment Type

This parameter only applies (and is made available) when the line type implements PRI_ISDN signaling (T1-PRI). This parameter defines which PRI ISDN signaling mode the MultiAccess is to run as. D_Channel signaling requires a Central Office to Premise Side relationship. The MultiAccess can operate as "TE connected to the public network" (default) or as "NT2 network side". NT2 could be used when the MultiAccess is connected to a PBX (or similar private equipment) that is already configured for premise side operation. When the MultiAccess is connected directly to a PRI line that is part of the public switched network, it should be set to TE.

Line Code

The Line Code parameter is a layer 1 technique used to identify and control the ones and zeros of the data pattern. T1 line codes are derived from the AMI (Alternate Mark Inversion) bi-polar technique. A voltage (pulse) on the digital line represents a binary one. No voltage represents a binary zero. The line code says each binary one must be of the opposite polarity with respect to the previous one (voltage alternating in polarity - the essence of a bipolar signal). The Line Type selection dictates the available Line Code choices.

When the line type is T1, your choices are:

Alternate Mark Inversion (AMI)

Line code is a bipolar coding scheme in which successive ones alternate in polarity. Successive ones of the same polarity are bipolar violations (BPV errors). BPVs and too many consecutive zeros are conditions that cause signal degradation. AMI line code requires user data to contain enough binary ones to maintain 1s density (signal integrity). The 1s Density rule is, in every 24 bits of information to be transmitted, there must be at least 3 ones (pulses) and that no more than 15 zeros can be transmitted consecutively.

Binary 8 Zero Substitution (B8ZS)

B8ZS (Binary 8 Zero Substitution). This line code is the same as AMI, except for when user data does not contain enough binary ones to maintain the "1s Density" rule). A "user" data stream of 16 consecutive zeros (to be transmitted) will be replaced with a B8ZS pattern (a pattern that contains a specific sequence of bipolar violations). The receiving end of this transmission will also be set to B8ZS line code and so when it recovers the specific pattern of violations, it will replace it with a string of zeros (transparently passing the data up to the receiving user as originally intended).

Receive Sensitivity

This layer 1 parameter configures (tunes) the interface's receiver circuit. There are two choices to select from, Short Haul Mode (-10db) and Long Haul Mode (-36 dB).

T1 signals are full duplex. A T1 digital interface generates and transmits a signal onto the line, while at the same time it receives and recovers a signal from the line.

Short Haul Mode (-10db)

Setting the receive sensitivity to Short Haul Mode means the MultiAccess receiver expects the size of the incoming signal to be between 0db and -10db. If the incoming signal is greater than 0db or if it's smaller than -10dB, the interface will indicate a Red Alarm condition.

Long Haul Mode (-36db)

Setting the receive sensitivity to Long Haul Mode means the MultiAccess receiver expects the size of the incoming signal to be between -10db and -36db. If the incoming signal is smaller than -36dB, the interface will not be able to recover it and will indicate a Red Alarm condition. If the incoming signal is greater than -10dB, depending on many variables (wave shape, jitter, dB level, cable quality, EMI, etc) erratic communication, bit errors and other problems may or may not result.

Country

This allows you to select the country for which the equipment is operating in and needs to comply with.

Line Build Out (LBO)

This layer 1 parameter dictates the physical size (decibel level) of the T1 signal being transmitted by the MultiAccess. Your choices are 0dB, -7.5dB, -15 dB & -22.5dB. 0dB is the largest size signal the MultiAccess can transmit.

There are a number of variables as to when the Line Build Out setting should be changed. The primary factors are, cable length, gauge and quality (twists per inch and shielding) and what size signal does the equipment opposite to the MultiAccess want to receive from the MultiAccess. As the signal travels down the cable it attenuates (becomes smaller and it's wave shape starts to change) - what size will it be at the other end of the cable?

If the receiving equipment (for example a T1 card in a PBX on your premise) is connected to the MultiAccess with a 6 foot cable, having the MultiAccess transmit at 0dB may be too hot (too large) of a signal for that device to receive, so setting the Line Build Out to -15dB may be more appropriate.

Voice Channel Encoding -

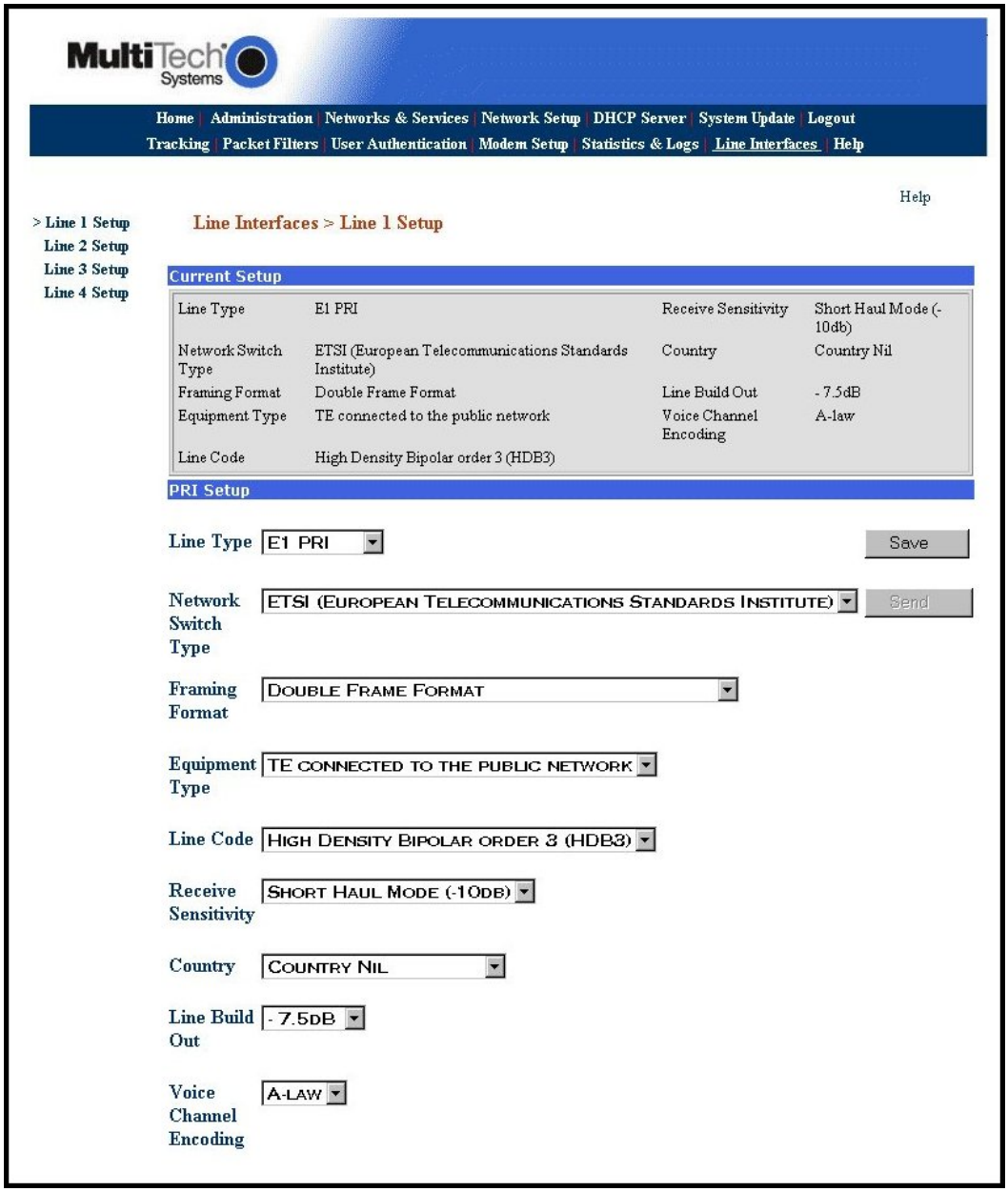
This parameter automatically follows the Line Type selection, however the user can change it from it's defaults. When the line type is set to E1, the PCM rule (Voice Channel Encoding) will be set to A-law. When the line type is set to T1, this option will be set to u-law. The ability to change this setting independent of the line type allows for flexibility in privately controlled closed circuit networks.

Line Interfaces > Line x Setup > E1 PRI

The Line Setup screen is made up of two fields, Current Setup (which displays the saved, active, settings) and Setup. The contents of the Current Setup field will not change until after the setup parameters have been properly loaded. The Setup field is used to load the parameters into the line interface. The parameters you select should match the parameters of the digital communication line provided by Telco.

The proper loading sequence is:

- Select the desired Line Type and wait for the screen to refresh (the available menu options will change based on the selected line type).
- Change any of the remaining options as needed.
- Click on the Save button and wait for the screen to refresh (the Send button will now be active).
- Click the Send button and wait for the screen to refresh (this takes approximately 45 seconds).
- Now the Current Setup field will reflect the new settings.


MultiTech Systems
Home | Administration | Networks & Services | Network Setup | DHCP Server | System Update | Logout
Tracking | Packet Filters | User Authentication | Modem Setup | Statistics & Logs | Line Interfaces | Help
Help
> Line 1 Setup
Line 2 Setup
Line 3 Setup
Line 4 Setup
Line Interfaces > Line 1 Setup
Current Setup
Line Type E1 PRI
Receive Sensitivity Short Haul Mode (-10db)
Network Switch Type ETSI (European Telecommunications Standards Institute)
Country Country Nil
Framing Format Double Frame Format
Line Build Out -7.5dB
Equipment Type TE connected to the public network
Voice Channel Encoding A-law
Line Code High Density Bipolar order 3 (HDB3)
PRI Setup
Line Type E1 PRI
Save
Network Switch Type ETSI (EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE)
Send
Framing Format DOUBLE FRAME FORMAT
Equipment Type TE CONNECTED TO THE PUBLIC NETWORK
Line Code HIGH DENSITY BIPOLAR ORDER 3 (HDB3)
Receive Sensitivity SHORT HAUL MODE (-10DB)
Country COUNTRY NIL
Line Build Out -7.5DB
Voice Channel Encoding A-LAW

Line Type

Three selections are available, T1-RBS, T1-PRI and E1-PRI. Units leave the factory set to E1-PRI. Line Interfaces that are activated in the field (when an MA30EXP port expansion module is installed) will default to T1-RBS. Whenever the line type setting is changed form E1-PRI to a T1 choice (or from a T1 choice to E1-PRI), after saving and sending the configuration change, the unit MUST be restarted. However, changing from T1-RBS to T1-PRI or changing any other parameter (for example the Framing Format or the Line Build Out) does NOT require a system reboot.

Network Switch Type

This parameter only applies (and is made available) when the line type implements PRI_ISDN signaling (E1-PRI). This parameter selects the specific messaging protocol that runs within the D_Channel between the Central Office switch and the MultiAccess.

Framing Format

The Framing Format parameter is a layer 1 parameter used to construct & identify the basic signal transmitted and received. The Line Type selection dictates the available formats.

When the line type is E1, your choices are:

- Double Frame Format,
- MultiFrame with Error Correction,
- MultiFrame with Extended Error Correction,

Equipment Type

This parameter only applies (and is made available) when the line type implements PRI_ISDN signaling (E1-PRI). This parameter defines which PRI ISDN signaling mode the MultiAccess is to run as. D_Channel signaling requires a Central Office to Premise Side relationship. The MultiAccess can operate as “TE connected to the public network” (default) or as “NT2 network side”. NT2 could be used when the MultiAccess is connected to a PBX (or similar private equipment) that is already configured for premise side operation. When the MultiAccess is connected directly to a PRI line that is part of the public switched network, it should be set to TE.

Line Code

The Line Code parameter is a layer 1 technique used to identify and control the ones and zeros of the data pattern. E1 line codes are derived from the AMI (Alternate Mark Inversion) bi-polar technique. A voltage (pulse) on the digital line represents a binary one. No voltage represents a binary zero. The line code says each binary one must be of the opposite polarity with respect to the previous one (voltage alternating in polarity - the essence of a bipolar signal). The Line Type selection dictates the available Line Code choices.

When the line type is E1, your choices are:

Alternate Mark Inversion (AMI)

Line code is a bipolar coding scheme in which successive ones alternate in polarity. Successive ones of the same polarity are bipolar violations (BPV errors). BPVs and too many consecutive zeros are conditions that cause signal degradation. AMI line code requires user data to contain enough binary ones to maintain 1s density (signal integrity). The 1s Density rule is, in every 24 bits of information to be transmitted, there must be at least 3 ones (pulses) and that no more than 15 zeros can be transmitted consecutively.

Binary 8 Zero Substitution (B8ZS)

B8ZS (Binary 8 Zero Substitution). This line code is the same as AMI, except for when user data does not contain enough binary ones to maintain the “1s Density” rule). A “user” data stream of 16 consecutive zeros (to be transmitted) will be replaced with a B8ZS pattern (a pattern that contains a specific sequence of bipolar violations). The receiving end of this transmission will also be set to B8ZS line code and so when it recovers the specific pattern of violations, it will replace it with a string of zeros (transparently passing the data up to the receiving user as originally intended).

High Density Bipolar of order 3 (HDB3)

line code is an AMI code working similar to B8ZS but with a much less tolerance for consecutive zeros. 4 consecutive zeros are substituted with an HDB3 pattern.

Receive Sensitivity

This layer 1 parameter configures (tunes) the interface's receiver circuit. There are two choices to select from, Short Haul Mode (-10db) and Long Haul Mode (-36 dB).

E1 signals are full duplex. An E1 digital interface generates and transmits a signal onto the line, while at the same time it receives and recovers a signal from the line.

Short Haul Mode (-10db)

Setting the receive sensitivity to Short Haul Mode means the MultiAccess receiver expects the size of the incoming signal to be between 0db and -10db. If the incoming signal is greater than 0db or if it's smaller than -10dB, the interface will indicate a Red Alarm condition.

Long Haul Mode (-36db)

Setting the receive sensitivity to Long Haul Mode means the MultiAccess receiver expects the size of the incoming signal to be between -10db and -36db. If the incoming signal is smaller than -36dB, the interface will not be able to recover it and will indicate a Red Alarm condition. If the incoming signal is greater than -10dB, depending on many variables (wave shape, jitter, dB level, cable quality, EMI, etc) erratic communication, bit errors and other problems may or may not result.

Country

This allows you to select the country for which the equipment is operating in and needs to comply with.

Line Build Out (LBO)

This layer 1 parameter dictates the physical size (decibel level) of the E1 signal being transmitted by the MultiAccess. Your choices are 0dB, -7.5dB, -15 dB & -22.5 dB. 0dB is the largest size signal the MultiAccess can transmit.

There are a number of variables as to when the Line Build Out setting should be changed. The primary factors are, cable length, gauge and quality (twists per inch and shielding) and what size signal does the equipment opposite to the MultiAccess want to receive from the MultiAccess. As the signal travels down the cable it attenuates (becomes smaller and it's wave shape starts to change) - what size will it be at the other end of the cable?

If the receiving equipment (for example a T1 card in a PBX on your premise) is connected to the MultiAccess with a 6 foot cable, having the MultiAccess transmit at 0dB may be too hot (too large) of a signal for that device to receive, so setting the Line Build Out to -15dB may be more appropriate.

Voice Channel Encoding - This parameter automatically follows the Line Type selection, however the user can change it from it's defaults. When the line type is set to E1 the PCM rule (Voice Channel Encoding) will be set to A-law. When the line type is set to T1 this option will be set to u-law. The ability to change this setting independent of the line type allows for flexibility in privately controlled closed circuit networks.

Chapter 4 - Troubleshooting

1. Verify that the site planning requirements are met. Refer to Chapter 2 of this manual.
2. Verify that the Administrations PC requirements are met (correct Default Gateway configuration, using an HTTPS-compatible Browser, JavaScript and Cascading Style active, and Proxies deactivated in the browser).
3. If you can't establish a connection and the message "***Error: The <software> is not reachable from the local network***" is displayed, try the following:
   - verify IP Addresses in the software are correctly configured (Chapter 3)
   - verify Default Gateway of the Client PC is correctly configured (Chapter 3)
   - verify proper Network Cable installation (Chapter 2)
4. Check for updates to the product documentation on the Multi-Tech web site at: http://www.multitech.com/DOCUMENTS/.
5. To troubleshoot TCP/IP connections in Windows 2000 use the **Ping**, **Tracert**, and **Pathping** commands. The Ping command sends an Internet Control Message Protocol (ICMP) packet to a host and waits for a return packet, listing the transit time. If there isn't a return packet, Ping indicates that with a Request Time Out message. The Tracert command traces the route between two hosts and can be useful in determining where in the route a communications problem is occurring. Windows 2000 provides the **Pathping** command, which combines the features of Ping and Tracert and adds additional features to help you troubleshoot TCP/IP connectivity problems.
7. If you are using an external keyboard connected to the MultiAccess's PC board using the **KB1** 6-pin female MiniDIN connector, make sure that you are not using an adapter cable (e.g., a 6-pin DIN to 6-pin miniDIN adapter cable).
8. Observe the MultiAccess front panel LEDs. Verify that the **LAN 1** and **LAN 2** LEDs indicate proper MultiAccess operation in terms of the Ethernet **LINK** integrity, transmit/receive activity (**ACT** LED), and speed (**100 MB**). Refer to the front panel LEDs description in Chapter 1 of this manual.
9. Attach a monitor and keyboard to the MultiAccess for monitoring and debugging (refer to Chapter 2 of this manual for keyboard and monitor connection information).
11. Run the applicable **Statistics & Logs** function for the MultiAccess's status and performance:
    - **Uptime:** length of continuous MultiAccess operation and date last booted
    - **Networks:** details of all interfaces, routing table, and current network connections to and from the system
    - **Modem Connections:** displays details of all modem connections
    - **Server Connections:** displays details of all server connections
    - **Interfaces:** graphically displays the network traffic on each interface, separated by days, weeks, months and years
    - **Accounting:** details of the traffic in bytes for each interface
    - **Self Monitor:** provides a record of processes which had to be restarted since they were abnormally terminated
    - **View Logs:** displays a list of log files maintained by the MultiAccess

    Refer to Chapter 3 of this manual for **Statistics & Logs** menu information.

Chapter 5 - MultiAccess Maintenance

This chapter covers issues related to routinely maintaining the MultiAccess, including:

- Housekeeping
- Monitoring

Housekeeping

Housekeeping includes the on-going list of tasks that you need to perform to keep your environment safe and clean. The three main housekeeping tasks that you'll need to revisit periodically are:

- **System backups** – This includes regular backups of MultiAccess configurations.
- **Accounts management** – Includes adding new accounts correctly, deleting old ones promptly, and changing passwords regularly. You should arrange to get termination notification when someone leaves your organization (e.g., for your company's full-time and contract employees, or your university's graduating students). This should involve maintaining current email addresses for alerts and notifications (e.g., from the **Administration** menu), as well as maintaining the overall WebAdmin password from the **Administration >Web Admin** menu.
- **Disk space management** – Includes timely 'cleanup' of random program and data files to avoid wondering if a program is a leftover from a previous user, or a required program needed for a new install, or a program that an intruder left behind as a 'present' for someone to open. Eliminating unneeded files will allow more room on the hard drive for important logs and reports.

Monitoring

Here you need to keep track of your system in terms of 'normal' usage so you can tell:

- If your MultiAccess is working.
- If your MultiAccess has been compromised.

To be proactive in solving these issues, keep track of usage reports and logs (refer to the sections on **User Authentication**, **Tracking**, and **Statistics & Logs** in Chapter 3).

Chapter 6- Warranty and Service

Warranty

Multi-Tech Systems, Inc., (hereafter "MTS") warrants that its products will be free from defects in material or workmanship for a period of two, five, or ten years (depending on model) from date of purchase, or if proof of purchase is not provided, two, five, or ten years (depending on model) from date of shipment.

MTS MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED.

This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by Customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory – transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES, AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PRICE FOR DEFECTIVE PRODUCTS.

Repair Procedures for U.S. and Canadian Customers

In the event that service is required, products may be shipped, freight prepaid, to our Mounds View, Minnesota factory:

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112
Attn: Repairs, Serial # _____

A Returned Materials Authorization (RMA) is not required. Return shipping charges (surface) will be paid by MTS.

Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), your telephone number, and if the product is out of warranty, a check or purchase order for repair charges.

For out of warranty repair charges, go to www.multitech.com/documents/warranties .

Extended two-year overnight replacement service agreements are available for selected products. Please call MTS at (888) 288-5470, extension 5308 or visit our web site at http://www.multitech.com/programs/orc/ for details on rates and coverages.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department at (800) 972-2439 or email tsupport@multitech.com. Please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at (800) 328-9717 or (763) 717-5631, or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Customers (Outside U.S.A. and Canada)

Your original point of purchase Reseller may offer the quickest and most economical repair option for your Multi-Tech product. You may also contact any Multi-Tech sales office for information about the nearest distributor or other repair service for your Multi-Tech product.
http://www.multitech.com/COMPANY/offices/DEFAULT.ASP

In the event that factory service is required, products may be shipped, freight prepaid to our Mounds View, Minnesota factory. Recommended international shipment methods are via Federal Express, UPS, or DHL courier services, or by airmail parcel post; shipments made by any other method will be refused. A Returned Materials Authorization (RMA) is required for products shipped from outside the U.S.A. and Canada. Please contact us for return authorization and shipping instructions on any International shipments to the U.S.A. Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), your telephone number, and if the product is out of warranty, a check drawn on a U.S. bank or your company's purchase order for repair charges. Repaired units shall be shipped freight collect, unless other arrangements are made in advance.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department nearest you or email tsupport@multitech.com. When calling the U.S., please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at +(763) 717-5631 in the U.S.A., or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Distributors

Procedures for International Distributors of Multi-Tech products are on the distributor web site at http://www.multitech.com/PARTNERS/login/ .

Copyright © Multi-Tech Systems, Inc. 2001

Regulatory Compliance

FCC Part 15 Regulation

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.
Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

FCC Part 68 Telecom

1. This equipment complies with Part 68 of the Federal Communications Commission (FCC) rules. On the outside surface of this equipment is a label that contains, among other information, the FCC registration number. This information must be provided to the telephone company.
2. As indicated below, the suitable jack (Universal Service Order Code connecting arrangement) for this equipment is shown. If applicable, the facility interface codes (FIC) and service order codes (SOC) are shown.
3. An FCC-compliant telephone cord with modular plug is provided with this equipment. This equipment is designed to be connected to the phone network or premises wiring using a compatible modular jack which is Part 68 compliant. See installation instructions for details.
4. The ringer equivalence number (REN) is used to determine the number of devices that may be connected to the phone line. Excessive REN's on the phone line may result in the device not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total REN's, contact the local phone company.
5. If this equipment causes harm to the phone network, the phone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the phone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
6. The phone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the phone company will provide advance notice in order for you to make necessary modifications in order to maintain uninterrupted service.
7. If trouble is experienced with this equipment (the model of which is indicated below) please contact Multi-Tech Systems, Inc., at the address shown below for details of how to have repairs made. If the equipment is causing harm to the network, the phone company may request that you remove the equipment from the network until the problem is resolved.
8. No repairs are to be made by you. Repairs are to be made only by Multi-Tech Systems or its licensees. Unauthorized repairs void registration and warranty.
9. This equipment should not be used on party lines or coin lines.
10. Manufacturer and device information:

Manufacturer:	Multi-Tech Systems, Inc.
Trade name:	MultiAccess ™
Model Numbers:	MultiAccess
FCC Registration Number:	US: AU7DDNAMA2496
Ringer Equivalence:	0.3B
Modular Jack:	RJ-11C or RJ-11W
Service Center in U.S.A.:	Multi-Tech Systems Inc. 2205 Woodale Drive Mounds View, MN 55112 (763) 785-3500 Fax (763) 785-9874

Canadian Limitations Notice

Notice: The ringer equivalence number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a phone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the ringer equivalence numbers of all the devices does not exceed 5.

Notice: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, phone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

EMC, Safety, and R&TTR Directive Compliance

The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility.

and

Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;

and

Council Directive 1999/5/EC of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Recording MultiAccess Information

Please fill in the following information on your Multi-Tech MultiAccess. This will help tech support in answering your questions. (The same information is requested on the Warranty Registration Card.)

Model No.: _____

Serial No.: _____

Software Version: _____

These numbers are located on the bottom of your MultiAccess. The Software Version is displayed at the top of the **Home** screen.

Provide the configuration information (e.g., Ethernet, gateway and other IP addresses used) from **Network Setup > Interfaces**, as well as any available **Statistics & Logs** information.

Record the Node ID# from the MultiAccess's back panel; it may be required by the ISP for administration purposes or connection identification. Every device that contains an Ethernet NIC (Network Interface Card) has an assigned Media Access Control (MAC) address to identify it and/or differentiate it from any other network-attached device.

Also, note the status of your MultiAccess including LED indicators, screen messages, diagnostic test results, problems with a specific application, etc.

Appendix A - License Agreements

This section provides the Multi-Tech Systems, Inc. End User License Agreement (EULA) as well as other applicable Licensing Agreements.

Multi-Tech Systems, Inc. End User License Agreement (EULA)

IMPORTANT - READ BEFORE OPENING THE SOFTWARE PACKAGE

This is a basic multi-user software license granted by Multi-Tech Systems, Inc., a Minnesota corporation, with its mailing address at 2205 Woodale Drive, Mounds View, MN 55112.

This is a legal agreement between you (either an individual or a single entity) and Multi-Tech Systems, Inc. for the Multi-Tech software product enclosed, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). The SOFTWARE PRODUCT also includes any updates and supplements to the original SOFTWARE PRODUCT provided to you by Multi-Tech.

Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement. By installing, copying, downloading, accessing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of that separate end-user license agreement.

This copy of Multi-Tech Systems software is provided only on the condition that you, Customer, agree to the following license agreement. READ THIS LICENSE CAREFULLY. If you do not agree to the terms contained in this license, return the packaged program UNOPENED to the place you obtained it. If you agree to the terms contained in this license, fill out the enclosed Software Registration Card, and return the card by mail. Registration may also be done on Multi-Tech Systems web site at www.multitech.com/register. Opening the packaged program constitutes agreement to be bound by the terms and conditions of this Software License Agreement. Your right to use the software terminates automatically if you violate any part of this software license agreement.

Multi-Tech Software License Agreement

Multi-Tech Systems, Inc. (MTS) agrees to grant and Customer agrees to accept on the following terms and conditions, a non-transferable and non-exclusive license to use the software program(s) delivered with this Agreement.

GRANT OF LICENSE. MTS grants Customer the right to use one copy of the software on a single product (the Licensed System). You may not network the software or otherwise use it on more than one product at the same time.

COPYRIGHT. The software is owned by MTS and is protected by United States copyright laws and international treaty provisions. Therefore, Customer must treat the software like any copyrighted material. Customer may install the software to a single hard disk and keep the original for backup or archival purposes. Customer shall NOT copy, or translate into any language, in whole or in part, any documentation which is provided by MTS in printed form under this Agreement.

OTHER RESTRICTIONS. The software may not be assigned, sublicensed, translated or otherwise transferred by Customer without prior written consent from MTS. Customer may not reverse engineer, decompile, or disassemble the software. Any updates shall be used only on the Licensed System, and shall remain subject to all other terms of this Agreement. Customer agrees not to provide or otherwise make available the software including, but not limited to documentation, programs listings, object code, or source code, in any form, to any person other than Customer and his employees and /or agents, without prior written consent from MTS. Customer acknowledges that the techniques, algorithms, and processes contained in the software are proprietary to MTS and Customer agrees not to use or disclose such information except as necessary to use the software.

Customer shall take reasonable steps consistent with steps taken to protect its own proprietary information to prevent the unauthorized copying or use by third parties of the software or any of the other materials provided under this Agreement. Any previous version of the software must be destroyed or returned to Multi-Tech Systems, Inc. within 90 days of receipt of the software upgrade or update.

LIMITED WARRANTY. MTS warrants that the software will perform substantially in accordance to the product specifications in effect at the time of receipt by Customer. If the MTS software fails to perform accordingly, MTS will optionally repair any defect, or replace it. This warranty is void if the failure has resulted from accident, abuse, or misapplication. A Software Registration Card must be on file at MTS for this warranty to be in effect. In all other respects, the MTS software is provided AS IS. Likewise, any other software provided with MTS software is provided AS IS. THE FOREGOING WARRANTY IS IN LIEU ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL MTS BE LIABLE FOR CONSEQUENTIAL DAMAGES RESULTING FROM USE OF THE LICENSED PROGRAM, WHETHER AS A RESULT OF MTS NEGLIGENCE OR NOT, EVEN IF MTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. MTS ALSO DISCLAIMS ANY LIABILITY IN CONTRACT OR OTHERWISE FOR THE DEFECT OR NON-PERFORMANCE OF ANY SEPARATE END-USER LICENSED SOFTWARE PRODUCT INCLUDED WITH MTS' SOFTWARE.

INDEMNIFICATION. MTS will indemnify and defend Customer from any claim that the software infringes on any copyright, trademark, or patent. Customer will indemnify and defend MTS against all other proceedings arising out of Customers use of the software.

GENERAL. If any of the provisions, or portions thereof, of this Agreement are invalid under any applicable statute or rule of law, they are to that extent deemed to be omitted.

This is the complete and exclusive statement of the Agreement between the parties, which supersedes all proposals, oral, written and all other communications between the parties relating to the subject matter of this Agreement. This Agreement may only be amended or modified in writing, signed by authorized representatives of both parties.
This Agreement shall be governed by the laws of the State of Minnesota.
The waiver of one breach or default hereunder shall not constitute the waiver of any subsequent breach or default. Licensee also agrees to the following:
I am not a citizen, national, or resident of, and am not under the control of the government of:
Afghanistan, Cuba, Iran, Iraq, Libya, Montenegro, North Korea, Pakistan, Serbia, Sudan, Syria, nor any other country to which the United States has prohibited export.
I will not download or by any other means export or re-export the Programs, either directly or indirectly, to the above countries, nor to citizens, nationals or residents of the above countries.
I am not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and/or Specially Designated Narcotics Traffickers, nor am I listed on the United States Department of Commerce Table of Denial Orders.
I will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists.
I will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical, or biological weapons of mass destruction.
Licensee agrees that by purchase and/or use of the Software, s/he hereby accepts and agrees to the terms of this License Agreement.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.
When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.
To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.
For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.
We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.
Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.
Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.
The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.
1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any

later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Appendix B – Modem Commands

This appendix describes the AT commands supported by the MultiAccess MA30120 modems along with application specific usage. The primary purpose of this appendix is for use with Customer specific inbound or outbound data applications that use the MultiAccess modems set to a usage of “Modem Sharing”.

COMPATIBILITY: The industry standard AT Command set, was devised to control the operation of standalone (traditional) modems. Such modems connect to the telephony network in the same way as a private telephone, with a ring detector and a hook relay. Their data connection is an RS-232 serial interface, with control signals such as DTR, RTS, DCD, and so on. Many of the functions associated with these traditional interfaces have no counterpart in the MA30120 modems. Wherever possible, support for common AT commands and S-Registers has been added with a view to ease of software compatibility. Please refer to section 3 of this appendix for additional details.

Note: Due to the nature of the Multi Access modems, user defined parameters (non factory defaults) must be issued to the modem before each call attempt.

The following sections within this appendix depict the AT commands supported by the MultiAccess.

1) AT Command Syntax Convention
2) Standard AT Commands Supported
3) Standard AT Commands Accepted with No Effect
4) S Registers
5) Advanced MultiAccess Modem Commands
6) Application Notes
7) ASCII Conversion Chart

“AT” Command Syntax Convention

“AT” Command Input Processing

In conformance to convention, the “AT” prefix is omitted from commands in the descriptions below. Thus, the answer command documented in the “AT Commands Supported” section as “A” would actually appear “ATA” if sent as a single command.

Commands may be chained, (directly concatenated) in which case the “AT” prefix should only precede the first command. For example, the command input string “ATE0V0” would both disable command echo and set the result code format to numeric.

All input command strings must be terminated by a carriage return (cr). Any line feed (lf) after the carriage return is ignored. The characters that the parser interprets as carriage return and line feed can be chosen as described in Parser Characters Settings.

The command “A/” is an exception to all three of the above rules in that it must *not* have an “AT” prefix, *cannot* be chained and must *not* be terminated by a carriage return, refer to “AT” Commands Supported.

Parser Character Settings

Certain characters used by the “AT” command parser and response generator are settable if the provided defaults are unsuitable. They can be changed via the appropriate S-register. The table below shows the semantics of the settable characters, the S-registers that hold them and the default values:

Settable Characters	S-Register	Default Value (Symbol)
Escape character	S2	43 (+)
Line Feed	S3	13 (\r)
Carriage Return	S4	19 (\n)
Backspace	S5	8 (\b)

Echo

By default, the “AT” command parser does not echo back command characters received from the host. Command mode echo can be enabled with the “E*n*” command as described in the “AT” Commands Supported.

Numerical Arguments to Commands

Many commands take a numerical argument immediately after the command character. For example “E*n*” accepts the numbers 0 and 1 for *n*. It is permissible to omit this argument, in which case the effect is the same as if the argument 0 had been supplied. For example “E” has the same effect as “E0”.

Result Codes

The “AT” command parser maintains a “result code”, which is set to “OK” at the start of command input string parsing. An invalid command in the input string causes the result code to be set to “ERROR”. The command being parsed is not executed. Any characters in the command input string after the error is detected are not parsed, so that any correctly constructed commands beyond the error are not executed. If no errors occur, the result code remains “OK”. The result code is sent to the host when the parser terminates, either by reaching the end of the command input string or by detecting an error. The format in which the result code is sent to the host may be controlled as described in the “Qn”, “Vn”, and “\Vn” in the “AT” Commands Supported.

Three commands are exceptions to the sending of the “OK” or “ERROR” result code. These are “ATA”, “ATD”, and “ATO”, refer to “AT” Commands Supported. Each of these commands itself terminates command input string parsing. They cause the modem to perform an action which is then reported by specific result codes such as “CONNECT”.

Null Command

The null command is permitted, has no effect and has an “OK” result code. A null command occurs when:

- the command input string consists only of the prefix “AT”
- the “A/” command is sent before any other command

Key-Press Abort

The key-press abort feature allows users to abort a call attempt after initiation, but before the link is established simply by pressing a character key on their terminal. Key-press abort is enabled upon receipt of an “A” (answer) or “D#” (dial) commands. Key-press abort is disabled when the modem reaches the Data state or enters the Terminating state having failed to establish the link. If any downstream data arrives at the modem from the host while key-press abort is enabled, then the modem will terminate the link. In addition, the result code “(ABORTED)” will be sent to the host prior to the usual “NO CARRIER” that occurs at link termination.

Escape Sequence Detection

When a modem is in the Data state (on-line\connected), downstream data (data transmitted from the host application via telnet to the MultiAccess) is passed over the dial up link to the peer system. The “AT” command processor may nevertheless still inspect this data looking for the “escape-to-command-mode” character sequence. If the sequence is detected, the modem will transition to the Command Escape state. Further downstream data will be directed to the “AT” command parser. Escape sequence detection consists of examining data sent to the modem from the user‘s host application for the character specified in S2 (‘+’ by default). Only if the buffer consists solely of one, two or three instances of this character does it contribute to

the escape sequence. If four or more octets are present or any of the characters are not the escape character, then escape sequence detection is restarted. The sequence is detected when exactly three escape characters have been collected. The figure below shows the only four possible sequences of buffers that result in escape sequence detection.

+ + +	+ + +	+ + +	+ + +

Sn=# Set the Value of an S-Register

The command "S*n*=#" enters the value # into S-register S*n*. This value is interpreted as a decimal number string and ends at the first character not in the range "0" to "9". The S-registers supported by the MultiAccess modems are described in the S-Registers section in this appendix. Registers not supported should not be accessed.

Sn? Query the Value of an S-Register

The command "S*n*?" returns the value of S-register S*n* in the response. The format of this response is a decimal number string both preceded and followed by a cr/lf sequence. This is followed by the usual "OK" result code. The S-registers supported by the MultiAccess are described in the S-Registers section in this appendix. Registers not supported should not be accessed.

"AT" Commands Supported

A/ Repeat Previous Command

The "A/" command causes the previous command input string to be re-parsed and commands re-executed exactly as before. This command must appear alone in a command input string and must *not* have an "AT" prefix. It does not require a carriage return since the parser begins re-parsing the previous command input string upon receipt of the '/' character.

A Answer a call

The "A" command causes the modem to answer. Any commands in the command input string appearing after the "A" command are ignored. This command may be chained after other commands, but it is not meaningful to chain other commands after it.

D<*string*> Dial a Number

The "D<*string*>" (dial command) causes the modem to proceed to originate mode. This command may be chained after other commands. The dial string is made up of two parts, the destination telephone number and optional dial modifiers. The total length of the dial string (including the "d") is 50 characters.

The characters after the command character 'D' are processed as follows:

All valid address digits and characters are processed in the order received. These characters are '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', '*' and '#'.

Two additional characters (the comma "," and the letter "R") are valid when the Modem Sharing option "Reverse Dial" option is enabled and when the t (tone) command immediately follows the d (dial) command in the dial string.

Commas add delay(s) to the call progress and are most commonly used when dialing a destination that initially answers with an automated attendant. For example, ATDT17637853500,,,,,5315 (with the 5315 being entered as the extension of the final destination).

The letter R instructs the MultiAccess modem to switch to answer mode after dialing. When the R is processed, it's echoed back to the host as a comma (for example: ATDT17637175038R is echoed back as ATDT17637175038,). See the Modem Usage section "Reverse Dial" found in Chapter 3 of the User's Guide, for complete details.

Dial modifier characters that are accepted but are discarded (have no function). These characters are 'P', 'W', '@', '!', ';', ')', '(', '-', ' ' (space), '"' and 'I'. The dial modifier t (tone command) is accepted but discarded when the Reverse Dial option is disabled.

All other characters cause the result code to be set to "ERROR" and the parser to abort.

E*n* Echo

This command controls the echoing of command characters back to the host.

"E0" disables echoing to host (DEFAULT setting as of version 1.12).

"E1" enables echoing to host.

H*n* Hang Up

The "H*n*" command causes the link to be terminated. The valid range of *n* is 0 to 1 but the value has no effect. This command is also accepted in the Idle state, but has no effect. The result code remains "OK".

I*n* Information

The "I*n*" command returns text to the host containing information about the MultiAccess modem devices. The valid range of *n* is 0 to 4.

"i0", "i2" and "i4" returns a basic identification of "Mapletree Networks UniPorte Architecture".

"i1" identifies which modem port of the total possible modems you are currently communicating with. "Port *n* of 0 to *m"* where *n* is the zero-based index of the port and *m* is the total number of ports. For example, "Port 0 of 0 to 29".

"i3" returns product information, including software versions, in the following format:

Performance Technologies, UniPorte Architecture Product Information
Country Code 001 - United States
V.92, V.90, K56flex, V.34bis, V.34, V.32bis, V.32, V.22bis
V.22, V.23, V.21, Bell 212, Bell 103, V.110
V.44, V.42, MNP2-4, V.42bis, MNP5
Fax Class 1, 1.0, 2, and 2.0
FoIP, VoIP
RISC Code Revision 01.10.00/f
RISC Revision Date 02/06/2005 (mm/dd/yyyy)
Build 014
DSP Code Revision 03.05.05/u
DSP Revision Date 06/02/2005 (mm/dd/yyyy)

Q*n* Quiet

The "Q*n*" command controls the sending of result codes to the host.
"Q0" enables the sending of all result codes.
"Q1" disables the sending of all result codes.
"Q2" enables the sending of all result codes in originate mode, but disables certain result codes in answer mode. This is the DEFAULT setting. Only "OK" "RING" and "ERROR" are sent in answer mode; other result codes such as "CONNECT", "NO CARRIER", etc. are not sent.

O*n* On-Line from Escape State

The "O*n*" command causes the modem to return to the Data state from the Command Escape state. A "CONNECT" result code will be sent to the host. User data flow, interrupted in the Command Escape state, will then resume. This command is only valid if the modem is in the Command Escape state. Otherwise, the above steps are *not* taken and the "ERROR" result code is set. The valid range of *n* is 0 to 1 but the value has no effect. Any commands in the command input string appearing after the "O*n*" command are ignored. This command may be chained after other commands, but it is not meaningful to chain other commands after it.

T Tone Dial

The "T" command is required use when the "reverse dial" option is enabled. If revese dial is disabled the tone command is accepted but has no effect.

V*n* Result Code Format

The "V*n*" command controls the format in which result codes are sent to the host.
"V0" – result codes are sent in numeric (short, terse) form
"V1" – result codes are sent in verbose (long, text) form (DEFAULT, restored by "Z" and "&F")

The following table shows the equivalence between numeric and verbose result code formats:

Numeric ("V0")	Verbose ("V1")				
0	OK	1	CONNECT	2	RING
3	NO CARRIER	4	ERROR	5	NO DIALTONE
6	BUSY	7	NO ANSWER	8	(ABORTED)
9	ERROR				

\Vn Extended Connect Message

The “\Vn” command controls the presentation of the connect message after the “CONNECT” result code. The valid range of n is 0 to 1. The default setting is 1. This parameter does not apply when the “Result Code Format” (V*n*) command is “Numeric” (V0).

“\V0” causes the “CONNECT” result code to consist only of the text “CONNECT”.

“\V1” causes the “CONNECT” (e.g., CONNECT 33600 /LAPM /V.42bis) result code to contain additional text specifying the bit rate, error-control protocol and compression protocol.

Z Reset to default Configuration

The “Z” command causes all configuration variables to be reset to the internal defaults, therefore this command has the same effect as “&F”. In addition, if the modem is in the Command Escape mode, the link is terminated.

&F Set to Default Configuration

The “&F” command causes all configuration variables for the modem to be immediately reset to the internal factory defaults.

Note: After every call attempt, the MultiAccess modem automatically returns to factory settings. After each call attempt, the user specific data application must re-initialize the modem to the desired parameters if the factory defaults are not sufficient for your application.

"AT" Commands Accepted with No Effect

This section lists the "AT" Commands that are accepted by the MultiAccess modems but have no effect. When they are met in the command input parser, any numerical argument is checked for validity, but it is otherwise ignored. The result code remains "OK" unless the numerical argument is out of range, in which case it is set to "ERROR". The following list also describes the normal use of the command used by a stand-alone modem connected to a POTS line.

L*n* Monitor Speaker Loudness

The "L*n*" command normally controls the monitor speaker volume. The valid range of *n* is 0 to 3.

M*n* Monitor Speaker Mode

The "M*n*" command normally controls when the monitor speaker is on. The valid range of *n* is 0 to 2.

P Pulse Dial

The "P" command normally changes the dialing mode to pulse.

&C*n* DCD Behavior

The "&C*n*" command normally controls the DCD handshake signal presented by a modem to the terminal. The valid range of *n* is 0 to 1.

&D*n* DTR Behavior

The "&D*n*" command normally determines the behavior of the modem when a terminal DTR transition to off is detected. The valid range of *n* is 0 to 3.

&K*n* Flow Control

The "&K*n*" command normally controls flow control. The valid range of *n* is 0 and 3 to 6.

&T*n* Loopback and Test

The commands "&T0" through "&T8" normally start and stop various loopback and test modes or control the response to requests for loopback from the peer modem. The valid range of *n* is 0 only. Other values set the result code to "ERROR" to reflect the fact that loopbacks and tests cannot be initiated by "AT" commands.

S0=n S Register 0

Normally used to control Auto Answer. Refer to S-Registers in the next section.

S-Registers

This section describes the S-Registers supported by the MultiAccess modems.

S0 Auto Answer

Compatibility: Superficial. Default: 1 Min: 0 Max: 255

In standalone modems, S0 is the number of ring cycles before automatic answer and, if zero, disables automatic answer. In the MultiAccess, upon the onset of ringing, the modem will not act until the “A” (answer) command is received from the User specific application. Traditional auto answer is not supported.

S2 Escape Character

Default: 43 ‘+’ Min: 0 Max: 127

This register defines the escape code character. The default character is the plus (+) sign (decimal 43). It may be set to any ASCII character, refer to the ASCII Conversion Chart at the end of this appendix. Setting a value greater than 127 results in no escape character, and therefore no means of entering command mode~~m~~ during on-line mode without breaking the on-line connection.

S3 Carriage Return Character

Default: 13 ‘\r’ (CTRL-M) Min:0 Max 127

This register defines the character recognized as the Carriage Return (Enter or Return Key). This register may be set to any ASCII character, refer to the ASCII Conversion Chart at the end of this appendix.

S4 Line Feed Character

Default: 10 ‘\n’ (CTRL-J) Min:0 Max 127

This register defines the character recognized as Line Feed. S4 may be set to any ASCII charater, refer to the ASCII Conversion Chart at the end of this appendix.

S5 Backspace Character

Default: 8 ‘\b’ (CTRL-H) Min: 0 Max: 127

This register defines the character recognized as Backspace. S5 may be set to any ASCII character, refer to the ASCII Conversion Chart at the end of this appendix.

S7 Connect Timeout

Unit Value: Seconds Default: 90 Min:0 Max 255

This register defines the abort timer (the time in which a connection must be established). In answer mode the timer starts upon receipt of the answer (a) command. In originate mode the timer starts upon execution of the dial command.

S11 DTMF Tone Duration

Unit Value: milliseconds Default: 70 Min: 50 Max: 255

This object defines the timing of transmitted DTMF digits. The value is the digit pulse width (on time) and inter-digit pause (off time) in milliseconds. The width and pause time cannot be defined independently.

S17 Error Correction Negotiation Timeout

Unit Value: 100 milliseconds Default: 150 Min: 0 Max: 255

This register defines how long, in units of 100ms, the modem will continue negotiation of an error control protocol. If the LAPM negotiation has not been completed within the specified time, the fallback action specified by S register 36, Error Correction LAPM Failure control, is taken. If a retrain occurs during this interval, the timer is restarted.

S19 Error Correction Retransmission Limit

Default: 12 Min: 0 Max: 255

This register controls the number of times that the modem will retransmit the same frame before disconnecting the link. When the modem is connected via V.90 modulation, the modem will attempt a retrain to the next lower V.90 speed rather than disconnecting. If the retrain is successful the connection will continue. Should a V.90 connection retrain to a V.34 modulation, the connection will continue as a V.34 connection. If the retransmit limit is reached while connected at a V.34 modulation, the modem will disconnect. A retransmit limit of 0 is used to denote no limit, indicating that a disconnect will not result regardless of the number of times a frame is retransmitted.

S20 Error Correction Maximum Frame Length

Default: 256 Min: 32 Max: 1024

This register limits the maximum frame length that will be offered during negotiation of an error control protocol. The modem may apply a smaller limit due to internal buffer space limitations and the final, effective frame length will, of course, be negotiated with the peer. The minimum packet size that can be negotiated is 32.

S23 LAPM Enabled in Originate Mode

Default: 1 Min: 0 Max: 1

This register controls whether the LAPM error control protocol is enabled in the originate mode.

If the value is 1, LAPM is enabled when originating a call. LAPM link requests will be sent (initiated) by the MA30120 modem, in accordance with S17 and S36.

If the value is 0, LAPM is disabled in the originate mode.

Note: In the answer mode, LAPM cannot be disabled. The MA30120 modem will always look for LAPM link requests in accordance with S50.

S36 Error Correction LAPM Failure Control

Default: 7Min: 0 Max: 7

This register defines the action taken if the primary error control protocol (LAPM) is disabled or cannot be established with the peer. The options are to disconnect (terminate the link), to establish a normal (non error-controlled) connection or to try to negotiate MNP error control. These are selected by this object's value as shown in the table below.

Value	Action on negotiate timeout
0	Disconnect
1	Establish a normal connection
2,3	Reserved
4	Try MNP2-4, disconnect if MNP fails
5, 6	Reserved
7	Try MNP2-4, then normal if MNP fails

S41 Data Compression Protocols Offered to Peer

Default: 7Min: 0 Max: 7

This register defines which Data Compression protocols are enabled. Data cannot be compressed without implementing Error Correction. LAPM, MNP and PIAFS are Error Correction protocols.

V.44 compression may be run over the LAPM error correction protocol only. If V.44 is enabled and can be negotiated with the peer during protocol negotiation. V.44 will take precedence over V.42bis.

V.42bis compression may be run over the LAPM, MNP and PIAFS error correction protocols.

MNP5 compression may be run only over an MNP error correction protocol. If during MNP protocol negotiation V.42bis is enabled and can be negotiated with the peer. V.42bis will take precedence over MNP5.

Value	Compression Offered
0	None
1	MNP5 Only
2	V.42bis Only
3	V.42bis and MNP5
4	V.44 Only
5	V.44 and MNP5
6	V.44 and V.42bis
7	V.44, V.42bis and MNP5

S47 Escape Sequence Detection in Call Mode

Default: 6Min: 5 Max: 6

This register controls the "AT" command parser that examines downstream data for the escape sequence. A value of 6 disables the escape sequence detection in answer mode and enables the escape detection in originate mode. A value of 5 enables the escape sequence detection for both answer and originate modes.

S50 Error Correction Auto Detection Timeout

Default: 50 (5 sec) Min:1 Max: 255

This register defines how long, in units of 100ms, a modem will attempt auto-detection of an error control protocol (in answer mode) before giving up and establishing a normal (non error-controlled) connection. During the auto-detection phase the modem will respond to an ODP sequence, HDLC flags, the configured fallback character, or MNP2 flags. If none of these are detected within the specified time, a normal link/connection is established.

S51 Error Correction Fallback Character

Default: 13 (‘\r’) Min: 0 Max: 127

This register defines the ASCII character that, if detected repeatedly (while in answer mode) is attempting auto-detection of an error control protocol, will cause the EC negotiation attempt to be abandoned and a normal (non error-controlled, asynchronous) link to be established. The character must be received three times consecutively. The default character is the Carriage Return (CR). The value of this register is in decimal.

Advanced MultiAccess Modem Commands

Advanced MultiAccess modem commands implement a unique syntax as compared to standard modem commands. The syntax includes ":m" & "index number" preceded by "at".
Format = AT:M*index# =value*

Companding Law

COUNTRY CODE Index 101 Default =1 (United States)

This index sets the companding law on the modem's telephony interface to either μ-law or A-law. The allowed values are defined below. The default country code is UNITED_STATES (having the value of 1) which selects μ-law companding. INTERNAT_MULAW and INTERNAT_ALAW have been provided for direct control of the companding law without the specification of a country. Where a country is known to have equipment operating with both laws, two entries are provided, e.g., KOREA_MULAW and KOREA_ALAW. There is no way to directly query the selected companding law, so it is very important to set this index with care.

μ-LAW		
UNITED STATES = 1	CANADA = 2	HONG KONG = 3
JAPAN = 4	KOREA MULAW = 5	TAIWAN = 6

INTERNAT MULAW = 15 (any μ-LAW country)
INTERNAT ALAW = 16 (any A-LAW country)

A-LAW		
ARGENTINA = 17	AUSTRALIA = 18	AUSTRIA =19
BELGIUM = 20	BRAZIL = 21	CHILE = 22
CHINA = 23	CYPRUS = 24	CZECH = 25
DENMARK = 26	DENMARK = 26	EGYPT = 27
FINLAND = 28	FRANCE = 29	GERMANY = 30
GREECE = 31	HOLLAND = 32	INDIA = 33
IRELAND = 34	ISRAEL = 35	ITALY = 36
KOREA ALAW = 37	MALAYSIA = 38	MEXICO = 39
NEW ZEALAND = 40	NORWAY = 41	PAKISTAN = 42
POLAND = 43	PORTUGAL = 44	RUSSIA = 45
SINGAPORE = 46	SOUTH AFRICA = 47	SPAIN = 48
SWEDEN = 49	SWITZERLAND = 50	SWITZERLAND = 50
THAILAND = 51	TURKEY = 52	UNITED KINGDOM=53

Call Types

Call Type Index 112 Default = 4 (Data Modem)

This index defines specific types of Analog or ISDN calls that can be made with the MA30120 system. Use this index appropriately if the desired type of connection is something other than the default. Appropriate use depends if the modem is answering an incoming call or originating an outbound call.

For inbound calls the Call Type index must preceed the “A” (answer) command within the same string.

To answer an incoming HDLC call issue “at:m112=32A”.

If the MultiAccess is to answer a standard analog data modem call, the answer command would simply be “ata” (including the Call Type index is NOT needed because Data Modem is the default call type).

For outbound calls, the Call Type index can be issued on a separate string, preceeding the dial string, or it can preceed the dial command as part of the same string.

If the MultiAccess is to dial out (originate) to a remote ISDN Terminal Adapter in HDLC mode, the initialization sequence would be as follows:

Configuration String = ate1q0:m112=32

Dial String = atdt*PHONENUMBER*

Or Together = atq0:m112=32dt*PHONENUMBER*

The possible values of the Call Type index (:m112=*n*) are as follows:

POS	=	2	(answer mode only)
Data Modem	=	4	(default)
ISDN V110	=	8	
ISDN PIAFS	=	16	
ISDN HDLC	=	32	
POS V22 Direct	=	64	(answer mode only)

CALL TYPE DEFINITIONS:

POS (Point of Sale) = The standard modulation handshake sequences will be used to establish carrier. The modem will be incapable of negotiating LAPM or MNP error correction. POS call Type is supported in the answer role only. The modem will connect in asynchronous mode (non -framed).

Data Modem = This is the default call type. Standard analog modem modulations (PCM) apply (i.e. V.92, V.90, V.34. V.32 etc). The modem will auto negotiate modulation protocols starting at V.92 and working down to Bell 103 along with auto negotiating error control protocls of LAPM or MNP and data compression protocols of V.44, V.42bis or MNP5. The modem will connect in asynchronous mode (non -framed).

ISDN V110 = V110 framed data operating directly on digital DS-0 channel. Auto rate-adaption of 19.2 kbps or slower. Associated with wireless calls.

ISDN PIAFS = A framed protocol operating directly on digital DS-0 channel for use in Japan. Associated with wireless calls.

ISDN HDLC = HDLC framed data operating directly on digital DS-0 channel at 64kbps.

POS V22 Direct = The connection is limited to V.22bis, V.22, Bell212, V.21 or Bell103. The modem will be incapable of negotiating LAPM or MNP error correction. This call type is supported in the answer role only. If the calling POS terminal is operating in synchronous SDLC mode, the port will detect the incoming flags (octet code 0x7E) and enter SDLC framed data transfer mode. Otherwise, the modem will enter asynchronous mode (non -framed). This call type allows the host to control many of the modulation handshake timing and operating parameters. Please see the POS V22 Direct Commands section later in this appendix regarding these additional parameters.

PLEASE NOTE: It is not necessary to change the Call Type index when using the modem to send or receive a FAX. The modem will switch to the appropriate FAX mode (Class 1, 1.0, 2 and 2.0) via standard *+FCLASS=#* commands.

However it is still necessary to include the +FCLASS=# command when answering an incoming FAX (for example at+fclass=2.0A).

FAX = Half duplex analog communication, incorporating multiple modulation protocols, transferring facsmile specific data. The MA30120 modems support Fax modes, Class 1, Class 1.0, Class 2 and Class 2.0.

Asynchronous Data Handling

The default asynchronous handling of data to be transmitted to the remote pier is 8 data bits, 1 stop bit and no parity. Asynchronous character handling can be configured to support any combination of the following:

7 or 8 data bits,
1 or 2 stop bits, and
No, Even, Odd, Space, Mark parity

The modem will perform parity insertion on transmission. The modem will not parity check the receive data but will pass the parity bit or stop bit to the host if it occupies the eighth bit position. For eight bits with parity the parity bit is not delivered to the host.

Three indexes are used to configure the asynchronous data format. Asynchronous data formats are not automatically detected. These parameters must be configured by the host prior to each call.

DATA BITS Index 252 Default = 8

This Index determines the number of data bits when connected in an asynchronous POS mode. The possible settings are 7 or 8 data bits. The default setting is 8 data bits.

STOP BITS Index 172 Default = 1

This index determines the number of stop bits when connected in an asynchronous POS mode. The possible settings are 1 or 2 stop bits. The default setting is 1 stop bit.

PARITY Index 219 Default = 0 (No Parity)

This index determines the parity of the data when connected in an asynchronous POS mode. The possible settings are as follows.

No Parity = 0 Even Parity = 1 Odd Parity = 2

Space Parity = 3 Mark Parity = 4

For Example: to configure the modem to use 7 Data Bits, 1 Stop Bit and Even Parity, issue:

AT:m252=7:m172=1:m219=1

Data Modem Commands:

Modulation Strap Index 256 Default = 0 (None)

This index selects a specific modulation (data modem analog protocol), limiting the physical connection to the advertised speed/protocol or slower. When the Modulation Strap is set to None, all supported analog protocols are advertised.

ModulationStrap NONE = 0,
ModulationStrap V90 = 1,
ModulationStrap K56 = 2,
ModulationStrap V34BIS_V34 = 3,
ModulationStrap V32BIS_V32 = 4,
ModulationStrap V22BIS_V22 = 5,
ModulationStrap V23 = 6,
ModulationStrap V21 = 7,
ModulationStrap BELL212_BELL103 = 8,
ModulationStrap H324_V34 = 9,
ModulationStrap H324_V90 = 10,
ModulationStrap BELL103 = 11,
ModulationStrap V22 = 12,

V.34 Bit Rate Restriction Index 270 Default = 13 (33600 bps)

This index selects the max allowable V.34 bit rate of the physical connection when the Modulation Strap of V34bis_V34 is selected. For instance, setting :m256=3:m270=10 will result in a 26400 speed connection or lower.

V34BitRateRestriction UNSPECIFIED = 0,
V34BitRateRestriction 4800 = 1,
V34BitRateRestriction 7200 = 2,
V34BitRateRestriction 9600 = 3,
V34BitRateRestriction 12000 = 4,
V34BitRateRestriction 14400 = 5,
V34BitRateRestriction 16800 = 6,
V34BitRateRestriction 19200 = 7,
V34BitRateRestriction 21600 = 8,
V34BitRateRestriction 24000 = 9,
V34BitRateRestriction 26400 = 10,
V34BitRateRestriction 28800 = 11,
V34BitRateRestriction 31200 = 12,
V34BitRateRestriction 33600 = 13,

V.92 Quick Connect Index 285 Default = 3 (Enabled)

This index is a feature that allows V92 clients to use previously obtained line quality configuration data to speed up portions of the negotiation process. Disabling this feature dictates the modems should use configuration data determined by a line probe during the negotiation process (for each call).

The supported values are:

V92 Quick Connect DISABLED = 0
V92 QuickConnect SHORT PHASE1 ONLY =1
V92 QuickConnect SHORT PHASE2 ONLY =2
V92 QuickConnect ENABLED =3

Enabling this feature (:m285=3) allows the V92 client to dictate configuration information used for both the V8 portion (phase 1) and the modulation portion (phase 2).

Note: Line conditions can change. With this feature enabled and if line conditions change, it could actually increase the connect time slightly.

V.8 Transmit Level Index 237 Default = 8992 (-9 dBm)

This index is used to set the transmit power for V.8. The default value of this index is a decimal value of 8992. The provided table shows index values for 1dBm increments from –9dBm to –20dBm.

-09dBm = 8992	-10dBm = 7301	-11dBm = 6507
-12dBm = 5799	-13dBm = 5168	-14dBm = 4806
-15dBm = 4105	-16dBm = 3659	-17dBm = 3261
-18dBm = 2906	-19dBm = 2590	-20dBm = 2308

Additionally, older slower protocols may perform better at higher power levels.

0 dBm = 23088	-03dBm = 16384	-05dBm = 12983	-07dBm = 10313

V.8BIS and V90 Control Index 115 Default = 2

V.8bis is used to negotiate K56Flex™ connections. V.8bis can also advertise V.90.

A value of 0 disables V.8bis.

A value of 1 enables V.8bis but without it advertising V.90.

A value of 2 enables the advertising of V.90 within V.8bis along with advertising K56Flex. This provides support for early implementations of V.90.

Please Note: Selecting a value of 0 or 1 does not disable the ability to establish V.90 connections, it simply changes where V.90 is offered within the negotiation process.

Answer State Delay Index 114 Default = 20

The minimum setting is 0. The maximum setting is 255.

This index is used to define the delay before entering into the answer state. The delay time is specified in 100 ms increments. The default value of 20 (times 100ms) equates to 2 seconds. This index would most likely be used in quick connect or reverse dial applications.

POS V22 Direct Commands

The following parameters within this section are available when the Call Type index is set to POS V22 Direct (:m112=64). The values of the following timing control parameters (indexes) are configured in milliseconds, but the DSP processing cycle occurs once every 6 ms. As a result, the timing that can be expected is as if the value is rounded up to the next higher 6 ms interval. A setting of 0 will result in a 6 ms interval.

Intercharacter Delay Index 253 Default = 0

The minimum setting is 0. The maximum setting is 255.

This index defines the intercharacter delay - meaning how long the modem waits for the next incoming character (coming from the line\remote POS) before it sends data in the upstream direction (to the host). If this index is set to zero (it's default), the intercharacter delay time is not active; pending upstream data will be delivered whenever there is no other data queued for processing in the upstream direction.

The units are in increments of 10 milliseconds. A value of 1 is the minimum. So at:m253=1 means the modem will wait up to 10 milliseconds for the next incoming character before it gives the data it has to the internal driver. If the remote POS connects at 2400 bps and sends 350 bytes, that means the modem in the MultiAccess will receive 1 byte every 4 milliseconds - so using :m253=1 means you should receive all 350 bytes at once.

Pause Before Answer Tone Index 173 Default 300

The minimum setting is 0. The maximum setting is 600.

This index defines in milliseconds how long the modem waits before it generates quick connect answer tones after it receieves the answer command.

Answer Tone Duration Index 174 Default = 660

The minimum setting is 0. The maximum setting is 1200.

This index defines the duration of the answer tone from the MultiAccess modem. The unit value is 1 millisecond. The default value is 660 milliseconds, The actual recommended minimum value is currently not known. We successfully tested with 100 milliseconds. Answer tone is traditionaly used to turn off the PSTN echo cancellors.

PAUSE AFTER ANSWER TONE Index 175 Default = 66

The minimum setting is 0. The maximum setting is 300.
This index controls the duration of the pause after the answer tone.

BELL212A V22 TX BINARY ONES DURATION Index 176 Default = 2400

The minimum setting is 0. The maximum setting is 4800.

This index controls the duration that the answering port transmits unscrambled binary ones while waiting to detect scrambled binary ones in Bell 212A and V.22 or the S1 sequence at V.22bis. Failure to detect scrambled binary ones within this time period will cause the port to fall back to V.21/Bell 103.

V22BIS TX DIBIT DURATION Index 178 Default = 84

The minimum setting is 0. The maximum setting is 360.

This index controls the length of time that the answering port transmits the V.22bis unscrambled repetitive double dibit pattern (S1) following detection of the S1 sequence from the client modem.

V22BIS TX BINARY ONES 1200 DURATION Index 179 Default = 444

The minimum setting is 0. The maximum setting is 600.

This index controls the length of time that the answering modem transmits scrambled-ones at 1200 bits/s following S1 detection during a V.22bis connection attempt.

BELL212A V22 TX BIN. ONES 1200 DURATION Index 180 Default = 6

The minimum setting is 0. The maximum setting is 300.

This index controls the length of time that the answering modem transmits scrambled-ones at 1200 bits/s during a Bell 212A or V.22 connection attempt.

V22BIS TX BINARY ONES 2400 DURATION Index 181 Default = 174

The minimum setting is 0. The maximum setting is 600.

This index controls the length of time that the answering modem transmits scrambled-ones at 2400 bits/s during a V.22bis connection attempt. The default value is 174 ms.

ANSWER TONE FREQUENCY Index 183 Default = 0

The minimum setting is 0. The maximum setting is 1.

This index controls the answer tone frequency. The possible settings are 0 and 1. If this index is set to 0, a 2100 Hz answer tone is sent. If it is set to 1, a 2225 Hz answer tone is set.

Application Notes

GENERAL

After each attempted call (answer or originate, successful or incomplete), the modem is automatically reset to factory default parameters.

Default modem operation and behavior:

Call type is analog Data Modem.
Auto answer is disabled (not supported).
V.92 enabled (auto negotiate fastest carrier rate possible with pier starting at V.92 and working it's way down to Bell 103).
V.44 enabled (Auto negotiate reliable connection with pier starting with V.44, then V.42, then Normal mode if reliable connection is not established within allotted variables).
Command mode Echo is disabled (E0 is set).
Extended result codes are enabled in Answer mode.
Result codes are disabled in Originate mode.
Escape Sequence is disabled in Answer mode.
Escape Sequence is enabled in Originate mode.

If, for inbound calls, the desired call type is to be something other than default, the call type command (index 112) must be issued with the "answer" command.

For Example:

Open the socket to the modem.
Initialize the modem (ate0q0).
Look for response "ok" (if applicable).
Look for the "ring" call progress message.
Issue the appropriate answer string.
For example, if the incoming call is an ISDN HDLC call, issue: at:m112=64a
Look for the call progress (connect 64000) message.
Look for, or start sending, application data

If, for outbound calls, the desired call type is to be something other than default, the call type command (index 112) must be precede the dial string (either as a separate command or chained with the dial string).

For Example, dialing out to a remote ISDN location:

Open the socket to the modem.
Initialize the modem (ate0q0).
Look for response "ok" (if applicable).
Issue the Call Type command followed by the dial string
at:m112=64
atd17635022020
or
at:m112=64d17635022020
Look for the call progress (connect 64000) message.
Look for, or start sending, application data

Data Modem - Connection Rate and Error Correction.

The MA30120 modem by default will auto negotiate the “carrier speed” (modulation protocol) and “type” (error control protocol) with the remote modem. The auto negotiation process starts at V92 speeds and works it way down to 300bps. The connection *type* refers to 1 of 2 basic methods of handling user data, with error correction or without it. A carrier without error correction is referred to as a “Normal” mode connection.

Applications that desire high speed modem connections (V.92, V90, V.34bis) and pass significant amounts of data (dial up Internet access) work best when the modems connect with error correction (V.44 or V.42). V.42 incorporates two methods of error correction (LAPM and MNP).

It may be benefical to use the Modulation Strap index to preset the speed at which the carrier negotiations start at.

Other applications may desire modem connections without error correction (normal mode connections). These types of application usually pass smaller amounts of data at slow rates (Point of Sale, ATM, proprietary data, etc, at 1200 or 2400 bps for example). Applications that desire normal mode connections may react differently to error control protocol negotiations and/or the time it takes to determine error correction will not be used. In certain situations it may be desirable to control or disable error control protocol negotiations (V.42).

Error correction commands mostly apply in both answer & originate modes, however some apply only in one mode.

In Answer mode, if the intention is to allow only V.42 type connections (LAPM or MNP), set S36 to a value of 4.

In Answer mode, if the intention is to allow only LAPM connection (disallow MNP or normal mode connections) set S36=0.

In Answer mode, if the intention is to force a normal mode connection with a remote modem that dials in with Auto Reliable mode enabled, set S50 to a value between 1 & 9 (depending on client modem variables). If the remote modem originates with error correction off, S50 controls how long the MultiAccess modem will wait before indicating connect. The minimum value for S50 is 1 (100 milliseconds).

In Originate mode, if the intention is to connect only with V.42 Error Correction (either via LAPM or MNP) set S36=4.

In Originate mode, if the intention is to connect only in Reliable MNP mode, disable LAPM with S23 = 0 and set S36=4.

In Originate mode, if the intention is to connect only in Normal mode (No Error Correction) regardless of client modem, set S23=0, S17=0, and S36=1.

ASCII Conversion Chart

CTRL	CODE	HEX	DEC	CODE	HEX	DEC	CODE	HEX	DEC	CODE	HEX	DEC
@	NUL	00	0	SP	20	32	@	40	64	`	60	96
A	SOH	01	1	!	21	33	A	41	65	a	61	97
B	STX	02	2	"	22	34	B	42	66	b	62	98
C	ETX	03	3	#	23	35	C	43	67	c	63	99
D	EOT	04	4	$	24	36	D	44	68	d	64	100
E	ENQ	05	5	%	25	37	E	45	69	e	65	101
F	ACK	06	6	&	26	38	F	46	70	f	66	102
G	BEL	07	7	'	27	39	G	47	71	g	67	103
H	BS	08	8	(	28	40	H	48	72	h	68	104`
I	HT	09	9	)	29	41	I	49	73	i	69	105
J	LF	0A	10	*	2A	42	J	4A	74	j	6A	106
K	VT	0B	11	+	2B	43	K	4B	75	k	6B	107
L	FF	0C	12	,	2C	44	L	4C	76	l	6C	108
M	CR	0D	13	-	2D	45	M	4D	77	m	6D	109
N	SO	0E	14	.	2E	46	N	4E	78	n	6E	110
O	SI	0F	15	/	2F	47	O	4F	79	o	6F	111
P	DLE	10	16	0	30	48	P	50	80	p	70	112
Q	DC1	11	17	1	31	49	Q	51	81	q	71	113
R	DC2	12	18	2	32	50	R	52	82	r	72	114
S	DC3	13	19	3	33	51	S	53	83	s	73	115
T	DC4	14	20	4	34	52	T	54	84	t	74	116
U	NAK	15	21	5	35	53	U	55	85	u	75	117
V	SYN	16	22	6	36	54	V	56	86	v	76	118
W	ETB	17	23	7	37	55	W	57	87	w	77	119
X	CAN	18	24	8	38	56	X	58	88	x	78	120
Y	EM	19	25	9	39	57	Y	59	89	y	79	121
Z	SUB	1A	26	:	3A	58	Z	5A	90	z	7A	122
[	ESC	1B	27	;	3B	59	[	5B	91	{	7B	123
\	FS	1C	28	<	3C	60	\	5C	92	|	7C	124
]	GS	1D	29	=	3D	61	]	5D	93	}	7D	125
^	RS	1E	30	>	3E	62	^	5E	94	~	7E	126
_	US	1F	31	?	3F	63	_	5F	95	DEL	7F	127

NUL Null, or all zeros
SOH Start of Header
STX Start of Text
ETX End of Text
EOT End of Transmission
ENQ Enquiry
ACK Acknowledge
BEL Bell or Alarm
BS Backspace
HT Horizontal Tab
LF Line Feed
VT Vertical Tab
FF Form Feed
CR Carriage Return
SO Shift Out
SI Shift In
DLE Data Link Escape
DC1 Device Control 1
DC2 Device Control 2
DC3 Device Control 3
DC4 Device Control 4
NAK Negative Acknowledge
SYN Sync.
ETB End Transmission Block
CAN Cancel
EM End of Medium
SUB Substitute
ESC Escape
S File Separator
GS Group Separator
RS Record Separator
US Unit Separator
DEL Delete

Appendix C – How to Update

There are two methods to update your MultiAccess: 1) Menu driven using the System Update on the Menu bar, and 2) the Manual Method described below.

Menu Driven:

If the IP address assigned to your MultiAccess has access to the Internet, the MultiAccess has a very user-friendly menu called “System Update”. Just click on the System Update link of the main menu bar. The update client within the MultiAccess will try to contact our MultiAccess Update Server via FTP. BE SURE TO READ THE NOTES listed on the web page for each update. All updates need to be applied sequentially (meaning a version can not be skipped). After selecting the desired update(s) - click the Apply button, your browser will be logged out and the unit will reboot.

MultiAccess units with version 1.09 or older contact the update server via directly opening the IP address 204.26.122.121. Starting with version 1.10 or newer it contacts the update server via the opening the DNS name “update.multitech.com”. For the MultiAccess to resolve DNS names, a valid DNS server must be defined in the Network Setup menu. As of March 2006 - The IP address of the Update Server is now 65.126.90.15. The FTP client within the MultiAccess is set to “active” mode.

MultiAccess Units running version 1.09 or older will need to manually updated to version 1.10 before it can use the menu driven method.

For the MultiAccess to have Internet Access - defining the appropriate Default Gateway in the “NetworkSetup” page is required.

Manual Method (via Linux command line):

Download the appropriate files via FTP from "update.multitech.com" (65.126.90.15).

When connecting to the update server via FTP, perform an anonymous login.

Username = anonymous

Password = any email address

There are two appropriate files per update/version; the primary file containing new files named with the format of “multiaccess-version.tar.gz”, and the corresponding .html file that contains the list of changes and version number used by HTTPD. Be sure the transfer mode is set to binary before getting\pulling down the files. Place the files in the appropriate directory (listed below) on the MultiAccess. The MultiAccess is an “FTP client” and is also an “SFTP client or server”. If you log into the MultiAccess as root at the command prompt, you can invoke ftp and open a connection to the update server. Or if you first put the files on a network server, you could use SFTP to push the files up to the MultiAccess.

General steps for a manual update, where the version level is incrementing by 1 (for example 1.06 to 1.07). In the following example X.XX is 1.07.

1. Place these files (multiaccess-X.XX.tar.gz and multiaccess-X.XX.html) into the /opt/multiaccess/htdocs directory.
2. Change to /opt/multiaccess/htdocs directory.
3. Apply the update with this command

   ruby /opt/multiaccess/ruby/updateclient.rb 1.1.1.1 apply multiaccess X.XX
4. Reboot the system with shutdown -r now (or cntl/alt/del)

General steps for a manual update, where the version level is incrementing by multiple versions (For example, updating a 1.06 unit to 1.10).

1. Place these files into the /opt/multiaccess/htdocs directory.

   multiaccess-1.07.tar.gz and multiaccess-1.07.html

   multiaccess-1.08.tar.gz and multiaccess-1.08.html

   multiaccess-1.09.tar.gz and multiaccess-1.09.html

   multiaccess-1.10.tar.gz and multiaccess-1.10.html

2. cd /opt/multiaccess/htdocs directory.

3. Apply each update one at a time with these commands (after issuing the command, wait for the prompt to return).

   ruby /opt/multiaccess/ruby/updateclient.rb 1.1.1.1 apply multiaccess 1.07

   ruby /opt/multiaccess/ruby/updateclient.rb 1.1.1.1 apply multiaccess 1.08

   ruby /opt/multiaccess/ruby/updateclient.rb 1.1.1.1 apply multiaccess 1.09

   ruby /opt/multiaccess/ruby/updateclient.rb 1.1.1.1 apply multiaccess 1.10

4. Reboot the system with shutdown -r now (or cntl/alt/del).

   Please Note: Read the update NOTES before applying the updates. There could be a unique variable for a particular update/patch that may have specific instructions to achieve the update, so read the contents of the html file/s before beginning. The update notes are from the perspective of using the "System Update" page to implement the update, so some notes may not apply or take on a different meaning when the updates are performed manually.

5. Attach a keyboard and monitor to the back of the unit. It can be helpful to watch system events as they occur.

   The updates may take a long time to down load and implement. Depending on the particular update, the implementation of it may occur upon the apply (step 3) & or the reboot (step 4).

Burning a New Hard Drive Image using the MultiAccess Recovery CD:

The MultiAccess ships with a Recovery CD. You need a keyboard and monitor connected to the MultiAccess and a CD-ROM drive that supports either a 40 pin IDE interface with an external power connection or a 44 pin IDE connection that uses power internal to the IDE cable. The MultiAccess provides extra power connections for use with 40 pin interfaces. The provided IDE cable is a 44 pin with a connector that converts to 40 pin (which can be removed).

When using a Recovery CD, the unit will be completely programmed back to factory settings, which includes among other things the following primary parameters:

LAN1 and LAN2 to 192.168.2.1 & 192.168.2.5 with a subnet mask of 255.255.255.000,

Modem Usage of RAS

Line Interface type will be set to T1-RBS.

Any User database (Local or RADIUS) defined within the unit will be lost.

The default factory accounts are administration only. The WEB administration account is admin/admin and the Linux root level account password is “linux”.

1. Power off the unit (properly shutdown the MultiAccess unit if possible). Consider disconnecting the Line Interface at the DMark\NIU. While the MultiAccess is down, your T1/E1 provider may require or desire the T1/E1 circuit to be looped back at the point of termination when the premise equipment is not providing a T1/E1 signal.

2. Remove the chassis cover by removing 3 screws across the back (center and outer ends). The cover slides forward approximately 1 inch, then lift straight up. The cover is on tight.

3. Connect Your CD-ROM drive to the extra IDE connection on the existing IDE Cable (noting the above details regarding 40 pin verses 44 pin). Do not remove the IDE Cable from the motherboard.

4. Insert the recovery CD into the CD-ROM drive and power-up the unit. The Unit will boot off the CD and prompt you to continue. When the process is finished, the CD-ROM drive will eject the disk and the unit will reboot. Depending on your CD-ROM drive, the disk tray will remain open while the MultiAccess boots up, or the tray may close again. Remove the disk while the tray is open or power off the unit before Linux starts to load.

Burning your own Recovery CD:

You can make your own recovery CD with the latest version by downloading the .iso file from the update server. Recovery images are named as "multiaccess-releasedate-v#.##.iso". For example the 1.11 version is named "multiaccess-01242005-v1.11.iso".

1. Download the image. Connect via FTP to update.multitech.com (204.26.122.121), login anonymously, set binary as the transfer mode and the get the .iso file. Note the exact size of the file as it is displayed on the update server. It should be the exact same size on your computer after you've downloaded it.

2. Once the file is on your computer, burn it as an "image" onto a blank CD.

Please Note: After downloading the .iso file from the update server, even though the file may be the correct size it is possible a portion of it may be corrupt (very unlikely but possible). If you wish, before burning it onto a CD you can use the appropriate .md5 file to verify the check sum of the .iso file. Copy the .md5 and .iso files (the files need to reflect the same version) to a temp directory on a linux/unix machine. Then from the temp directory issue the command "md5sum -c filename.md5", for example "md5sum -c multiaccess-01242005-v1.11.md5".

Appendix D – Waste Electrical and Electronic Equipment (WEEE) Statement

July, 2005

The WEEE directive places an obligation on EU-based manufacturers, distributors, retailers and importers to take-back electronics products at the end of their useful life. A sister Directive, ROHS (Restriction of Hazardous Substances) complements the WEEE Directive by banning the presence of specific hazardous substances in the products at the design phase. The WEEE Directive covers all Multi-Tech products imported into the EU as of August 13, 2005. EU-based manufacturers, distributors, retailers and importers are obliged to finance the costs of recovery from municipal collection points, reuse, and recycling of specified percentages per the WEEE requirements.

Instructions for Disposal of WEEE by Users in the European Union

The symbol shown below is on the product or on its packaging, which indicates that this product must not be disposed of with other waste. Instead, it is the user's responsibility to dispose of their waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or where you purchased the product.

Glossary

*** (Asterisk character)** – The 'wildcard' character, used to signify "all within this group or function" (e.g., use ***** to specify all domain names). A special symbol that stands for one or more characters. Many operating systems and applications support wildcards for identifying files and directories. This lets you select multiple files with a single specification. For example, in DOS and Windows, the asterisk (*) is a wild card that stands for any combination of letters.

: (colon character) – The character used by the MultiAccess™ Communications Server Web Management software for a port range. For example, to enter the S-Port/Client source port number as a port range, enter 1024:64000.

, (comma character) – The character used by the MultiAccess™ Communications Server Web Management software for a list of port numbers. For example, to enter the S-Port/Client source port numbers as a list of port numbers, enter 25, 80, 110.

- (dash character) – An acceptable MultiAccess™ Communications Server Web Management entry field character. For example, from **Radius > Secret** you can enter a shared **Secret** using alphanumeric characters, the dash (**-**) or the space or underline (_) characters.

_ (space or underscore character) – An acceptable MultiAccess™ Communications Server Web Management entry field character. For example, from **Radius > Secret** you can enter a shared **Secret** using alphanumeric characters, the dash (**-**) or the space or underline (_) characters.

Alias – A name, usually short, easy to remember is translated into another name, usually long and difficult to remember.

Anonymous FTP – Anonymous FTP allows a user to retrieve documents, files, programs, and other archived data from anywhere in the Internet without having to establish a user ID and password. By using the special user ID of "anonymous" the network user will bypass local security checks and will have access to publicly accessible files on the remote system.

ARP (Address Resolution Protocol) – An IETF standard that allows an IP node to determine the hardware (datalink) address of a neighboring node. ARP provides a method of converting Protocol Addresses (e.g., IP addresses) to Local Network Addresses (e.g., Ethernet addresses). ARP exists as a low-level protocol within the TCP/IP suite and is used to "map" IP addresses to Ethernet (or other) addresses (i.e., ARP provides the physical address when only the logical address is known).

Attack – An attempt at breaking part or all of a cryptosystem; can be either a successful or unsuccessful attempt. Many types of attacks can occur (e.g., algebraic attack, birthday attack, brute force attack, chosen ciphertext attack, chosen plain text attack, known plain text attack, linear cryptanalysis, and middleperson attack).

Authentication – The action of verifying information such as identity, ownership or authorization. Authentication is a security process where user access is allowed only if user authentication verifies the identity of the user requesting access to network resources. Authentication is one of the functions of IPSec. Authentication establishes the integrity of a data stream, ensures that it is not tampered with in transit, and confirms the data stream's origin. Authentication establishes the legitimacy of users and defines the allowed parameters of the session they establish.

Broadcast – The address that a computer refers to if it wants to address all the computers of a network. Example: for a network with the IP address 212.6.145.0 and a net mask 225.225.225.240, a broadcast would be the address 212.6.145.15.

CSS (Cascading Style Sheets) – HTML was intended to mark up only a Web page's structure, but not its on-screen display characteristics. For Web page appearances, the World Wide Web Consortium (W3C) developed a complementary markup system called Cascading Style Sheets (CSS) to make it easier to define a page's appearance without affecting its HTML structure. HTML can be frustrating when trying to control the appearance of a Web page and its contents. Style sheets work like templates: you define the style for a

particular HTML element once, and then use it over and over on any number of Web pages. To change how an element looks, you just change the style; the element automatically changes wherever it appears. (Before CSS, you had to change the element individually, each time it appeared.) Style sheets let Web designers more quickly create consistent pages and more consistent web sites.
Browsers began supporting the first CSS Specification, Cascading Style Sheets, Level 1 (CSS1), in versions 3.0 of Opera and Microsoft Internet Explorer and in version 4.0 of Netscape Navigator. The 4.0 and later versions of all three browsers also support properties from the newer Cascading Style Sheets, Level 2 (CSS2) specification, which let you specify elements' visibilities, their precise positions on the page, and how they overlap each other.

Certificate – A cryptographically signed object that contains an identity and a public key associated with the identity. Public key certificates are digital stamps of approval for electronic security. The three main characteristics of certificates are: 1) provide identification of the web site and the owner, 2) contain the public key to be used to encrypt and decrypt messages between parties, and 3) provide a digital signature from the trusted organization that issued the certificate, as well as when the certificate expires.

Certificate Authority – The issuer of a certificate is the Certificate Authority (CA). The CA is the party that digitally signs a certificate and ensures its validity. There are two types of CAs, private and public. Private CAs issue certificates for use in private networks where they can validate the certificate. Public CAs issues certificates for servers that belong to the general public. A Public CA must meet certain requirements before they are added as a root authority to a browser. Since this is a controlled process, all public CA must be registered to issue certificates.

Certificate Revocation List – A log of certificates that have been revoked before their expiration date.

Cipher – An encryption/decryption algorithm.

Ciphertext – Encrypted data.

Client-Server Model – A common way to describe the paradigm of many network protocols. Examples include the name-server/name-resolver relationship in DNS and the file-server/file-client relationship in NFS.

CHAP (Challenge Handshake Authentication Protocol) – An IETF standard for authentication using PPP which uses a "random Challenge", with a cryptographically hashed "Response" which depends on the Challenge and a secret key.

Client – A client is a program that communicates with a server via a network, so as to use the service provided by that server. Example: Netscape is a www client, with the help of which one can call up information from a www server.

Client-Server Principle – Applications based on the client-server principle use a client program (client) at the user-end that exchanges information with a server on the network. Usually the server is responsible for the data keeping, while the client takes over the presentation of this information and the interaction with the user. For this, the server and the client employ an exactly defined protocol. All the important applications in the Internet (e.g. www, FTP, news) are based on the client-server principle.

CMP (Certificate Management Protocol) – A protocol defining the online interactions between the end entities and the certification authority in PKI. It is written by PKIX working group of IETF and is specified in document RFC 2510.

Compromise – The unintended disclosure or discovery of a cryptographic key or secret.

CRL – Certificate Revocation List.

Cryptography – The art and science of using mathematics to secure information and create a high degree of trust in the networking realm. See also public key, secret key.

CSR (Certificate Signing Request) – The form used to obtain a certificate from a CA. A CSR generates a formatted certification. This request is located on the web site of all certificate authorities. Another way to generate a CSR is to use a utility such as Microsoft IIS or OpenSSL.

Datagram – The unit of transmission at the ISO Network layer (such as IP). A datagram may be encapsulated in one or more packets passed to the data link layer. A datagram is a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.

Default Route – A routing table entry that is used to direct packets addressed to networks not explicitly listed in the routing table.

DES (Data Encryption Standard) – A secret key encryption scheme; contrast with “public key”. DES is an NIST standard for a secret key cryptography method that uses a 56-bit key.

Destination Port Number ZZZZ – All the traffic going through the firewall is part of a connection. A connection consists of the pair of IP addresses that are talking to each other, as well a pair of port numbers. The destination port number often indicates the type of service being connected to. When a firewall blocks a connection, it will save the destination port number to its logfile.
Port numbers are divided into three ranges:

- The Well-Known Ports are those from 0 through 1023. These are tightly bound to services, and usually traffic on this port clearly indicates the protocol for that service. For example, port 80 virtually always indicates HTTP traffic.
- The Registered Ports are those from 1024 through 49151. These are loosely bound to services, which means that while there are numerous services "bound" to these ports, these ports are likewise used for many other purposes. For example, most systems start handing out dynamic ports starting around 1024.
- The Dynamic and/or Private Ports are those from 49152 through 65535. In theory, no service should be assigned to these ports.

DHCP (Dynamic Host Configuration Protocol) – An IETF standard for dynamically allocating and managing a pool of IP addresses, allowing a smaller number of addresses to serve a much larger number of users.

Digital Signature – The encryption of a message digest with a private key. Digital signatures are based on public-key cryptography, which was first introduced by Whitfield Diffie and Martin Hellman of Stanford University in 1976. Until 1976 there was only conventional cryptography, which uses the same key to both scramble (encrypt) and unscramble (decrypt) information. Public key cryptography is based on two keys, a private key and a public key.
Where conventional cryptography is a one-key system for both locking (encrypting) and unlocking (decrypting) a message, public key cryptography uses different keys for locking and unlocking.
In public-key systems, one key can be kept private while the other key is made public. Knowing the public key does not reveal the private key.

DNAT (Dynamic NAT) – Used to operate a private network behind a firewall and make network services that only run there available to the Internet.
The use of private IP addresses in combination with Network Address Translation (NAT) in the form of Masquerading, Source NAT (SNAT), and Destination NAT (DNAT) allows a whole network to hide behind one or a few IP addresses preventing the identification of your network topology from the outside. With these mechanisms, Internet connectivity remains available, while it is no longer possible to identify individual machines from the outside. By using Destination NAT (DNAT), it is still possible to place servers within the protected network/DMZ and make them available for a certain service.
In DNAT, only the IP address – not the port – is translated. Typically, the number of externally visible IP addresses is less than the number being hidden behind the NAT router.

DNS (Domain Name System) (also **Domain Name Service**) – Refers to the more user-friendly names, or aliases instead of having to use computer-friendly IP addresses. Name servers take care of the conversion from number to name. Every institution connected to the Internet must operate at least two independent name servers that can give information about its names and numbers. Additionally, there is a name server for every top-level domain that lists all the subordinate name servers of that domain. Thus the Domain Name System represents a distributed hierarchical database. Normally, however, the database is not accessed by the user him-/herself, but by the network application that he/she is presently working with.

DDoS (Distributed Denial of Service) – Attacks are a nefarious extension of DoS attacks because they are designed as a coordinated attack from many sources simultaneously against one or more targets. See also "DoS attacks".

DoS (Denial of Service) attacks – A major concern to the Internet community because they attempt to render target systems inoperable and/or render target networks inaccessible. DoS attacks typically generate a large amount of traffic from a given host or subnet and it's possible for a site to detect such an attack in progress and defend themselves. See also "Distributed DoS attacks".

Encapsulation – The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. For example, in Internet terminology, a packet would contain a

header from the physical layer, followed by a header from the datalink layer (e.g., Ethernet), followed by a header from the network layer (IP), followed by a header from the transport layer (e.g. TCP), followed by the application protocol data.

Encryption – A form of security wherein readable data is changed to a form that is unreadable to unauthorized users. Encryption involves the conversion of data into a secret code for transmission over a public network. The original (plain) text is converted into coded form (called cipher text) using an encryption algorithm. The cipher text is decoded (decrypted) at the receiving end, and is converted back into plain text.

ESP (**Encapsulating Security Payload**) – An authentication protocol much like AH. IP ESP may be applied in combination with AH. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. ESP may be used to provide the same security services as AH, plus it provides an encryption service. The main difference between the ESP authentication method and the AH authentication method is that ESP does not protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode). ESP is important for the integrity and encryption of datagrams.

Expiration Date – Certificates and keys may have a limited lifetime, and expiration dates are used to monitor and control their useful life.

Filter – A set of rules that define what packets may pass through a network. Filters can use source, destination, or protocol to determine whether to pass or discard a packet transmission. Part of a packet (the header) must contain information that matches the information in the defined rules or else the packet filter will discard it.

Filtering – The act or process of defining which data traffic is to be allowed between the network and hosts, typically using packet filter rules. Filtering is the central part of firewall security. With packet filter rules, you define which data traffic is allowed between the networks and hosts. You can also define particular packets to be filtered and are not to be allowed to pass through the firewall. Several types of filtering exist (e.g., Protocol filtering, port number filtering, URL address filtering, and IP address filtering).

Finger – Windows NT and 2000 have a TCP/IP utility called **Finger**. This utility is an old TCP/IP tool (very popular on UNIX systems) that matches an email address with the person who owns it and provides information about that person. While the Finger utility is fairly old (there are more advanced tools available that performs the same general function), it still works and can be a useful tool in certain situations.

The Finger utility was actually developed as the Finger Information Protocol. Finger was designed to provide an interface to the Remote User Information Program (RUIP). RUIP provides information about users who have accounts on UNIX-based computer networks. The Finger utility was created six years before the Internet was born. The first documentation on the Finger utility was in IETF RFC742, dated December 1977. A popular slogan promoting the phone book's yellow pages was "Let your fingers do the walking". The utility was christened "Finger", since the utility was basically designed for tracking down people.

The Finger Information Protocol let UNIX users on college campuses create a profile, called a "Plan page", which included personal and job-related information. A Plan page was similar to a personal home page on the Internet today. So when someone "Fingered" your email address, they learned more about you. The Finger utility is a command line tool, so in Windows NT or Windows 2000 you must first access a command-prompt window to use it. You then type the command followed by an email address.

Firewall – A device that serves to shield and thus protect a (partial) network (e.g., MultiAccess) from another network (e.g. the Internet). The entire network traffic runs via the firewall where it can be controlled and regulated. Technically this can be achieved in different ways. The use of special hardware firewalls is rare. More frequent is the use of routers with firewall options. The most common is use of firewall software on a specially dedicated computer.

Gateway – A combination of hardware and software that links two different types of networks. E.g., gateways between email systems allow users on different email systems to exchange messages.

Hacker – A person who tries to, and/or succeeds at defeating computer security measures.

Hacking Lexicon – The terms used by hackers; entire dictionaries exist to document hacking terms (e.g., http://www.robertgraham.com/pubs/hacking-dict.html). These documents clarify many of the terms used within the context of information security (infosec).

Hash – A one-way security function that takes an input message of arbitrary length and produces a fixed-length digest. Used in SHA (Secure Hash Algorithm).

Header – The portion of a packet, preceding the actual data, containing source and destination information. It may also error checking and other fields. A header is also the part of an electronic mail message that precedes the body of a message and contains, among other things, the message originator, date and time

Host – In client-server architectures, the computer on which the server software is running is called the host. It is possible for several servers to be running on one host, e.g. one FTP server and one email server. Hosts can be accessed with the help of clients, e.g. with a browser or an email program. As the expression *server* is used for the program (i.e. the software) as well as for the computer on which the program is running (i.e. the hardware), *server* and *host* are not clearly separated in practice. In data telecommunication the computer from which information (such as FTP flies, news, www pages) is fetched, is called the host. A host is also called a node in the Internet. Using an Internet host (as opposed to a local host), it is possible to work from a distance (remote access).

Host – A computer that allows users to communicate with other host computers on a network. Individual users communicate by using application programs, such as electronic mail, Telnet, and FTP.

HTTPS (aka, **S-HTTP)** – Secure HyperText Transfer Protocol, a secure way of transferring information over the World Wide Web. HTTPS refers to the entry (e.g., https://192.168.2.100) used for an S-HTTPS connection. S-HTTPS is the IETF RFC that describes syntax for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web. S-HTTP provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-reputability of origin. S-HTTP emphasizes maximum flexibility in choice of key management mechanisms, security policies and cryptographic algorithms by supporting option negotiation between parties for each transaction.

ICMP – The **Internet Control Message Protocol** notifies the IP datagrams sender about abnormal events. ICMP might indicate, for example, that an IP datagram cannot reach an intended destination, cannot connect to the requested service, or that the network has dropped a datagram due to old age. ICMP also returns information to the transmitter, such as end-to-end delay for datagram transmission.

IETF (**Internet Engineering Task Force**) – The international standards body that has standardized the IP protocol and most of the other successful protocols used on the Internet. The IETF web page is at http://www.ietf.org/.

IP – The **Internet Protocol** (IP) is the basic protocol for the transmission of Internet information. It has been in use virtually unchanged since 1974. It establishes and ends connections, as well as recognizing errors. By using NAT and Masquerading, private networks can be mapped onto official IP addresses. This way, the Ipv4 address space will still last a long time. Standard Internet open protocols include:

Protocol	Function
TCP/IP	basic network communication
HTTP	browsing
NFS	File Service
IMAP4/SMTP	Mail Service
DNS	Naming Service
DNS/LDAP	Directory Services
Bootp/DHCP	Booting Services
SNMP	Network Administration

IP Address – A 32-bit number that identifies the devices using the IP protocol. An IP address can be unicast, broadcast, or multicast. See RFC 791 for more information. Every host has a clear IP address, comparable with a telephone number. An IP address consists of four decimal numbers between 1 and 254 divided by dots (e.g., a possible IP address is 212.6.145.0. At least one name of the form xxx belongs to every IP address (e.g. xxx). This defines a computer with the name ox that is in the sub domain xxx of the sub domain xxx of the domain xxx. Like with IP addresses, the individual name parts are divided by dots. However, as opposed to IP addresses, IP names are not limited to four parts. Also, several IP names can be assigned to one IP address; these are referred to as aliases.

IP Header – The part of the IP packet that carries data used on packet routing. The size of this header is 20 bytes, but usually the IP options following this header are also calculated as header. The maximum length of the header is 60 bytes. The header format is defined in RFC 791.

IP Packet – A self-contained independent entity of data carrying sufficient information to be routed from the source to the destination computer without relying on any earlier exchange between this source and destination computer and the transporting network. The Internet Protocol (IP) is defined in RFC 791.

IP Payload – The part of the IP packet that carries upper level application data.

Key – A data string which, when combined with source data (packet) using a special algorithm, produces output that cannot be read without that specific key. Key data strings are typically 40-168 bits in length.

Key Agreement – A process used by two or more parties to agree upon a secret symmetric key.

Key Exchange – A process used by two more parties to exchange keys in cryptosystems.

Key Generation – The act or process of creating a key.

Key Management – The various processes that deal with the creation, distribution, authentication, and storage of keys.

Key Pair – Full key information in a public-key cryptosystem; consists of the public key and private key.

L2TP (Layer Two Tunneling Protocol) – A security protocol that facilitates the tunneling of PPP packets across an intervening network in a way that is highly-transparent to both end-users and applications. L2TP is defined in IETF RFC 2661.

LILO (LInux LOader) – LILO is a small program that sits on the master boot record of a hard drive or on the boot sector of a partition. LILO is used to start the loading process of the Linux kernel. (There are other programs that can also do this, such as **grub**. Most distributions / versions of Linux use LILO.) You can set up lilo to require a password to start to load the Linux kernel, or you can set it up to require a password if you want to pass any extra options to the Linux kernel before it starts loading.

Mapping – Logically associating one set of values (such as addresses on one network) with values or quantities on another set (such as devices on another network). Examples include name-address mapping, inter-network route mapping, and DNAT port mapping. Name resolution (name to address mapping) is another example.

Masquerading – The concealing of internal network information (LAN) form the outside. For example, the computer of a colleague with the IP address is inside a masked network. All the computers inside his network are assigned one single, official IP address (i.e. if he starts an HTTP request into the Internet, his IP address is replaced by the IP address of the external network card). This way, the data packet entering the external network (Internet) contains no internal information. The answer to the request is recognized by the firewall and diverted to the requesting computer.

MD5 (Message Digest 5) – A one-way hashing algorithm that produces a 128-bit hash. It computes a secure, irreversible, cryptographically strong hash value for a document. The MD5 algorithm is documented in IETF RFC 1321.

Message Digests – Mathematical functions (aka, one-way hashes) that are easy to compute but nearly impossible to reverse. The message digest serves as a "fingerprint" for data. As such, it is an element of most data security mechanisms (e.g., Digital Signatures, SSL, etc.). The hashing function takes variable-length data as input, performs a function on it, and generates a fixed-length hash value.

MPPE (Microsoft Point-to-Point Encryption) – An encryption technology developed by Microsoft to encrypt point-to-point links. The PPP connections can be over a VPN tunnel or over a dial-up line. MPPE is a feature of Microsoft's MPPC scheme for compressing PPP packets. The MPPC algorithm was designed to optimize bandwidth utilization in supporting multiple simultaneous connections. MPPE uses the RC4 algorithm, with either 40-bit or 128-bit keys, and all MPPE keys are derived from clear text authentication of the user password. The MultiAccess supports MPPE 40-bit/128-bit encryption.

Name Resolution – The process of mapping a name into its corresponding address.

NAT (Network Address Translation) – IP NAT is comprised of a series of IETF standards covering various implementations of the IP Network Address Translator. NAT translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet.

Netfilter – The Linux packet filter and network address translation (NAT) system that aims to reduce the number of filter points and to separate the filtering function from the NAT function. Netfilter is derived from the Linux **ipchains** and the Unix **ipfilter** packet filtering systems. The MultiAccess uses a Linux 2.4 kernel (and, for example, **iptables** for the internal logic in the netfilter code).

Network Card – The Ethernet PC card used to connect the MultiAccess to the internal, external or DMZ network (aka: NIC or NIC card).

NIC (**Network Interface Card**) – The Ethernet PC card used to connect the MultiAccess to the internal, external or DMZ network (aka, Network Card).

Nslookup – A Unix program for accessing name servers. The main use is the display of IP names for a given IP address and vice versa. Beyond that, other information can also be displayed (e.g., aliases).

Packet Filter – An operation that blocks traffic based on a defined set of filter "rules" (e.g., IP address or port number filtering).

PCT (**Private Communications Technology**) – A protocol developed by Microsoft that is considered more secure than SSL2. (Note that some web sites may not support the PCT protocol.)

PING (**Packet InterNet Groper**) – A program to test reachability of destinations by sending an ICMP echo request and waiting for a reply. The term is also used as a verb: "Ping host X to see if it is up."

PKI (**Public Key Infrastructure**) – Consists of end entities that possess key pairs, certification authorities, certificate repositories (directories), and all of the other components, software, and entities required when using public key cryptography.

Plaintext – Information (text) which has not been encrypted. (The opposite is ciphertext.)

Port – Where as only the source and target addresses are required for transmission on the IP level, TCP and UDP require further characteristics to be introduced that allow a differentiation of the separate connections between two computers. A connection on the TCP and UDP level are thus clearly identified by the source address and the source port, as well as by the target address and the target port.

Port Range – A series of TCP or UDP port numbers that can be set in MultiAccess protocol service definitions. For example, when adding a service from **Networks & Services > Services**, enter the source (client) port. The entry options are a single port (e.g. 80), a list separated by commas (e.g. 25, 80, 110), or a port range (e.g. 1024:64000).

Port Scanning – Attempting to find "listening" UDP or TCP ports on an IP device, and then obtaining information about the device. Portscanning itself is not harmful, but hackers to allow intrusion by brute-force password guessing can use it.

PPP (Point-to-Point Protocol) – An IETF standard which provides a method for transporting multi-protocol datagrams over point-to-point links. All of the users on the Ethernet connection share a common connection, so the Ethernet principles supporting multiple users in a LAN are combined with the principles of PPP, which typically apply t serial connections.

PPPoE (Point-to-Point Protocol over Ethernet) – An IETF standard which provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator. To provide a point-to-point connection over Ethernet, each PPP session must learn the Ethernet address of the remote peer, as well as establish a unique session identifier.

PPTP (Point-To-Point Tunneling Protocol) – A protocol that allows secure remote access too corporate networks (VPNs) over the Internet. All data sent over a PPTP connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, IPX) can be run concurrently. **Note**: the MultiAccess does NOT support IPX or Netbeui when using PPTP tunneling.

Protocol – A clearly defined and standardized sentence of commands and answers, with whose help a client and a server can communicate. Well-known protocols and the services they provide are, for example, HTTP (www), FTP (ftp), and NNTP (news).

Proxy (Application Gateway) – The task of a proxy (Application Gateway) is to completely separate the communication connections between the external network (Internet) and the internal network (LAN). There must be no direct connection between an internal system and an external computer. The proxies work exclusively on the application level. Firewalls that are based on proxies use a dual homed gateway that does not transfer any IP packets. The proxies that run as specialized programs on the gateway can now receive connections for a special protocol, process the received information at the application level and then transfer them.

Proxy ARP – The technique in which one machine, usually a router answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP allows a site to use a single IP address with two physical networks. Subnetting would normally be a better solution.

Private Key – In public key cryptography the private key is only known to the holder and it can be used to sign and decrypt messages.

Proxy – A cache server that acts as a firewall, protecting the local network. It allows an application inside the proxy to access resources on the global Internet.

PSK (Pre Shared Key) – A PSK password must be entered at both ends of the VPN tunnel. This password is also called the secret. The holder of this password can establish a VPN connection to the secure network. Make sure that this password does not reach the wrong hands and that you change the PSK password at regular intervals.

Public Key – In public key cryptography the public key, which is included in the certificate, can be used to verify signatures and encrypt messages. A sample public key is shown below:

```
0sAQNic1Tww7iknvNd6ieKDhd9JTu/Krbc71H4oIFd/xqKJntU8x25
M0Wbxr0gQngECdZPWHj6KeSVtMtslzXMkxDecdawoCadPtPiH/lln
23GKUOt3GoDVMob+fob9wBYbwdHOxPAYtNQBxNPEU9PGMxQd
Yp8io72cy0duJNCXkEVvpvYvVzkmp0xVYOWYkfjiPsdhnz5FCitEh6
XsCe0ctByoLjKA1C+mLtAlWhuycVojr2JwzSqUIJXzS6nV4yrpI+QY5
o5yztgjVIgwW1Er6jyyo2aeFLgucqjuHSZ+sX0dz/OfdQ0N0AjRAmO3
eknOYLk2DPRkmUeYr3W95q1Z2j/+4GRlzzP8ZoyPwdBv7hpZ0TRA
9c38a26+La8N2/TDKx+fGLfixB6Ed8X0jCmq4lt7iD2d/9EWeaUZfctq
aKfw==
```

Public key cryptography is based on two keys, a private key and a public key. Where conventional cryptography is a one key system for both locking (encrypting) and unlocking (decrypting) a message, whereas public key cryptography uses different keys for locking and unlocking. In public-key systems, one key can be kept private while the other key is made public. Knowing that the public key does not reveal the private key.

PuTTY – A simple but excellent ***SSH*** and ***Telnet*** replacement for Windows 95/98/NT that happens to be free. Installation is simple - you download ***PuTTY.exe*** and store it somewhere on your system that's convenient.

Qmail – A security-oriented Unix mailer daemon developed by Dan Bernstein.

RADIUS – RADIUS stands for **Remote Authentication Dial-In User Service**. RADIUS is a protocol with which the router can obtain information for the user authentication from a central server.

RFC (Request For Comments) – A document of Internet Society under standardization. See also IETF.

RFC 921 – A policy statement on the implementation of the Domain Style Naming System on the Internet. RFC 921 details the schedule for the implementation for the Domain Style Naming System in terms of 1) the names themselves, 2) the method of translating names to addresses, and 3) the relationship between the Internet and the rest of the world.

RFC 953 – The official IETF specification of the Hostname Server Protocol, a TCP-based hosts information program and protocol. The function of this server is to deliver machine-readable name/address information describing networks, gateways, hosts, and eventually domains, within the Internet environment. To access this server from a program, establish a TCP connection to port 101 (decimal) at the service host, SRI-NIC.ARPA (26.0.0.73 or 10.0.0.51).

RFC 1918 – An IETF standard for Address Allocation for Private Internet.

Router (**Gateway**) – A router is a device that selects intelligent pathways for network packets. Strictly speaking, a gateway is something different than a router, but in connection with TCP/IP, both terms are synonyms. To establish connections throughout world and not just stay within one's own network, one has to introduce this router (gateway) to one's computer. Normally, the highest address on the network 134.93.178.0 is the address 134.93.179.254 (since 134.93.179.255 is the broadcast). Generally, a router is a node that forwards packets not addressed to itself. Requirements for a router are defined in IETF RFC 1812.

RSA – A public key encryption and digital signature algorithm. It was invented by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm was patented by RSA Security, but the patent expired in September 2000.

Rsync – A synchronization protocol that uses checksums to determine differences (as opposed to using modification dates) and does a partial file transfer (transferring only the differences instead of entire files). **Rsync** was developed by Andrew Tridgell and Paul Mackerras; the **rsync** daemon (***rsyncd***) provides an efficient, secure method for making files available to remote sites.

Rules – The configuration settings used to set how packets are filtered. The rules are set with the network and service definitions set up in the **Networks & Services** menu. When setting packet filter rules, the two basic types of security policies are:

1. All packets are allowed through – the rules setup must be informed explicitly what is forbidden.
2. All packets are blocked – the rules setup needs information about which packets to let through. This lets you explicitly define which packets may pass through the filter. All other packets are blocked and can be displayed for viewing. See also "Filtering".

SCP (Secure copy) – The main purpose of SCP is the safe copying of files between local and remote computers. The MultiAccess supports login using SCP. A Windows SCP client can be downloaded from http://winscp.vse.cz/eng/. WinSCP is freeware SCP client for Windows 95/98/2000/NT using SSH (Secure shell). WinSCP manages some other actions with files beyond the basic file copying function.

Secret Key – The key used both for encryption and decryption in secret-key cryptography.

Secure Channel – A communication medium that is safe from the threat of eavesdroppers.

Seed – A random bit sequence used to generate another, usually longer, pseudo-random bit sequence.

Security Policy – Enterprises should have a carefully planned set of statements in place regarding network protection. A good corporate Internet security policy should define acceptable use, acceptable means of remote access, information types and required encryption levels, firewall hardware and software management processes and procedures, non-standard access guidelines, and a policy for adding new equipment to the network. New security protocols, new services, and security software upgrades should also be considered. The purpose of a security policy is to define how an organization is going to protect itself. The policy will generally require two parts: a general policy and specific rules (system specific policy). The general policy sets the overall approach to security. The rules define what is and what is not allowed. The security policy describes how data is protected, which traffic is allowed or denied, and who is able to use the network resources.

Server – A server is a device on the network that provides mostly standardized services (e.g., www, FTP, news, etc.). To be able to use these services, you as a user require the comparable client requirements for the desired service.

SHA (Secure Hash Algorithm) – A United States government standard for a strong one-way, hash algorithm that produces a 160-bit digest. See MD5. SHA-1 is defined in FIPS PUB 180-1.

SHA-1 (**Secure Hash Algorithm version one**) – The algorithm designed by NSA, and is part of the U.S. Digital Signature Standard (DSS).

S-HTTP (Secure HTTP) – The IETF RFC that describes a syntax for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web.
Secure HTTP (S-HTTP) provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-reputability of origin. The protocol emphasizes maximum flexibility in choice of key management mechanisms, security policies, and cryptographic algorithms by supporting option negotiation between parties for each transaction. The current IETF RFC describes S-HTTP version 1.2. Previous versions of S-HTTP numbered 1.0 and 1.1 have also been released as Internet-Drafts.

SNAT (Source NAT) – A functionality equivalent to DNAT, except that the source addresses of the IP packets are converted instead of the target address. This can be helpful in more complex situations (e.g., for diverting reply packets of connections to other networks or hosts). In contrast to Masquerading, SNAT is a static address conversion, and the rewritten source address does not need to be one of the firewall's IP addresses. To create simple connections from private networks to the Internet, you should use the Masquerading function instead of SNAT.
The use of private IP addresses in combination with Network Address Translation (NAT) in the form of Masquerading, Source NAT (SNAT), and Destination NAT (DNAT) allows a whole network to hide behind one or a few IP addresses preventing the identification of your network topology from the outside. With these mechanisms, Internet connectivity remains available, while it is no longer possible to identify individual machines from the outside. Using DNAT makes it possible to place servers within the protected network and still make them available for a certain service.

SOCKS – A proxy protocol that allows the user to establish a point-to-point connection between the own network and an external computer via the Internet. Socks, also called Firewall Transversal Protocol, currently exist at version 5.

Stateful Inspection – A method of security that requires a firewall to control and track the flow of communication it receives and sends, and to make TCP/IP-based services decisions (e.g., if it should accept, reject, authenticate, encrypt and/or log communication attempts). To provide the highest security level possible, these decisions must be based on the Application State and/or the Communication State (as opposed to making decisions based on isolated packets). With stateful inspection, a firewall is able to obtain, store, retrieve, and manipulate information it receives from all communication layers as well as from other applications. Stateful inspection tracks a transaction and verifies that the destination of an inbound packet matches the source of a previous outbound request. Other firewall technologies (e.g., packet filters or application layer gateways) alone may not provide the same level of security as with stateful inspection.

Static Route – A directive in a node that tells it to use a certain router or gateway to reach a given IP subnet. The simplest and most common example is the default router/gateway entry entered onto any IP-connected node (i.e., a static route telling the node to go to the Internet router for all subnets outside of the local subnet).

Subnet Mask – The subnet mask or the net mask indicates into which groups the addresses are divided. Based on this arrangement, individual computers are assigned to a network.

Syslog – A service run mostly on Unix and Linux systems (but is also available for most other OSes) to track events that occur on the system. Other devices on the network may also be configured to use a given node's syslog server to keep a central log of what each device is doing. Analysis can often be performed on these logs using available software to create reports detailing various aspects of the system and/or the network.

TCP (Transmission Control Protocol) – A widely used connection-oriented, reliable (but insecure) communications protocol which is the standard transport protocol used on the Internet. TCP is defined in IETF RFC 793.

Telnet – The Internet standard protocol for remote terminal connection service. It is defined in IETF RFC 854 and extended with options by many other RFCs.

TLS (Transport Layer Security) – An open security standard that is similar to SSL3. (Note that some web sites may not support the TLS protocol.)

Trace Route – A program available on many systems that traces the path a packet takes to a destination. It is mostly used to debug routing problems between hosts. A Trace Route protocol is defined in IETF RFC 1393.

Trusted Subnetwork – A subnetwork of hosts and routers that can trust each other not to engage in active or passive attacks. It is also assumed that the underlying communications channel such as a LAN is not being attacked by any other means.

Tunneling – Transmitting data that is structured in one protocol within the protocol or format of a different protocol.

UDP (User Datagram Protocol) – An datagram-oriented unreliable communications protocol widely used on the Internet. It is a layer over the IP protocol. UDP is defined in IETF RFC 768.

UNC (Universal Naming Convention) path – A UNC path (e.g., \\server) is used to help establish a link to a network drive.

URL (Universal Resource Locator) – URLs are used to describe the location of web pages, and are also used in many other contexts. An example of an URL is http://www.ssh.com/ipsec/index.html. URLs are defined in IETF RFCs 1738 and 1808.

Verification – The act of recognizing that a person or entity is who or what it claims to be.

VLAN (Virtual Local Area Network) – A function allowing some Ethernet switches to be divided into smaller logical groups known as VLANs. On most switches each VLAN operates completely independent of the others, as if each was a separate physical device. Some higher-end switches can also route between VLANs as if each was a separate hub/switch connected by a router.

VPN (Virtual Private Network) – A device or program that protects users and their data when exchanging information over the Internet. A VPN can use encryption, user authentication, and/or firewall protection to solve remote access security threats.

WAN (Wide Area Network) – A data network, typically extending a LAN beyond a building or campus, linking to other (remote) LANs.

Index

A

Accounting 70
Add a Network 50
Add Services 53
Administration 17
Administration > Intrusion Detection 45
Administration > Site Certificate 41
Administration > SNTP Client 38
Administration > SSH Client 37
Administration > System Setup 35
Administration > Tools 47
Administration > WebAdmin 39

B

Back Panel 8, 14
Broadcast
  on one network segment 73
  on whole Internet 72

C

COM1 jack 8
Connecting a Workstation to the RouteFinder 15

D

DHCP Server 17, 66
DHCP Server > Subnet Settings 66
DNAT 64
DNAT 64

E

E1/PRI interfaces 5

F

Features 6
Front Panel 7

G

Glossary 166
GNU General Public License 138

H

Hardware Installation 14
Help 17
Home 17
Host name 19
Housekeeping 130
HTTPS port 40

I

ICMP forwarding 74
Intrusion Detection 45
IP Aliases 59

L

Licenses
  GNU General Public License 138
  Multi-Tech Systems, Inc. End User License Agreement . 136
Line Interfaces 17
LINE jack 8
Login 15
Logout 17, 34

M

Maintenance 130
Masquerading 61
Modem Setup 17
Monitoring 130
MultiAccess Communications Server 5
Multi-Tech Systems, Inc. End User License Agreement 136

N

Network Card configuruation 58
Network Groups 54
Network Setup 17, 19
Network Setup > DNAT 64
Network Setup > Interfaces 56
Network Setup > Masquerading 61
Network Setup > SNAT 63
Networks 50
Networks & Services 17
Networks & Services > Network Groups 54
Networks & Services > Networks 50
Networks & Services > Service Groups 55
Notification by Email 36
Notificiation, types of 36

P

Packet Filter Rules 71
Packet Filters 17
Packet Filters > Packet Filter Rules 71
Password Changing 40
POWER Switch 8
Protocol
  AH 52
  ESP 52

ICMP 52
TCP & UDP 52

R

Rack Installation 12
RADIUS 80
Recording RouteFinder Information 135
Regulatory Information 133
Repair Procedures 131
RF660VPN software 32
Rules 71

S

Safety 12
Service Groups 55
Setup Your Time Zone 18
Ship Kit 6
Site Certificate 41
SNAT 63
Specifications 11
SSH Client 37
Starting up the RouteFinder 15
Statistics & Logs 17
Statistics & Logs > Uptime 100
Subnet Settings 66
System Setup 35
System Update 17

T

T1/E1 PRI ISDN 5
T1/E1/PRI line jacks 8
T1/PRI interfaces 5
T1/RBS 5
Tools 47
Traceroute 48
Tracking 17
Tracking > Accounting 70

U

Uptime 100
USB 8
User Authentication 17
User Authentication > RADIUS 80
User Defined Packet Filter Rules 72

V

V.92 remote access server (RAS) 5
VIDEO jack 8

W

Warranty 131
WebAdmin 39